State Identity Credential and Access Management (SICAM)

Roadmap and Implementation Guidelines

Version .5
Publication Date: **DRAFT**
TRM_1.5.885.002

September 16, 2010

Revision History

REVISION HISTORY			
REVISION/WORKSITE #	**DATE OF RELEASE**	**OWNER**	**SUMMARY OF CHANGES**
TBD	3/26/2010	Lee Mosbrucker	Initial Draft Release
Version .2	6/5/2010	Lee Mosbrucker	Convert CA- state specific to General State positions
Version .2.2	6/21/2010	Micheline Casey	Added assurance level information, risk assessment methodology, added suggested sections
Version .3	9/9/2010	Stephan Papadoulos	Added updated goal summary graphic, reorganized goals and objectives section and included maturity model summary
Version.4	9/14/2010	Lee Mosbrucker Gary Dias	Include Vendor Data Points and reformat
Version .5	9/16/2010	Lee Mosbrucker Gary Dias	Include roadmap and implementation sections.

Approvals

NAME	ROLE	DATE

EXECUTIVE SUMMARY

The State Identity and Credential Access Management (SICAM) Roadmap outlines a strategic vision for identity, credential, and access management efforts and emphasizes the importance of implementing the SICAM architecture and services in support the challenges associated with Trust, Interoperability, Security, and Process Improvement.

There are multiple initiatives working to address these challenges – Personal Identity Verification (PIV) cards are being issued in increasing numbers, the Public Key Infrastructure (PKI) has connected government and commercial PKIs via a trust framework and working groups are tackling relevant questions for mission-specific functions.

This document was developed to provide a common architecture and implementation guidance for use by State and local Agencies as they continue to invest in Identity and Access Management (IAM) programs. The IAM architecture will serve as an important tool for providing awareness to external mission partners and drive the development and implementation of interoperable solutions.

Contents

1. INTRODUCTION

1.1 Background

As part of a nationwide movement toward proactive citizen service delivery, transparency, and accountability, States are increasing sharing and utilization of data between departments, counties, and the federal government. Programs like the US Department of Education's P-20 State Longitudinal Data Systems (SLDS), require the ability to track a student's performance and the specific factors (e.g., educational programs, teachers, schools) that influenced outcomes from Preschool to age 20 (P-20),. To meet the SLDS requirement, student data must be analyzed from the multiple State departments that deliver educational services, including Human Services, K-12 Education, Workforce Development, Corrections, and Higher Education. Similarly, States are being asked to measure and report the outcomes of other federally funded programs around health, job creation, voting, welfare, and nutrition.

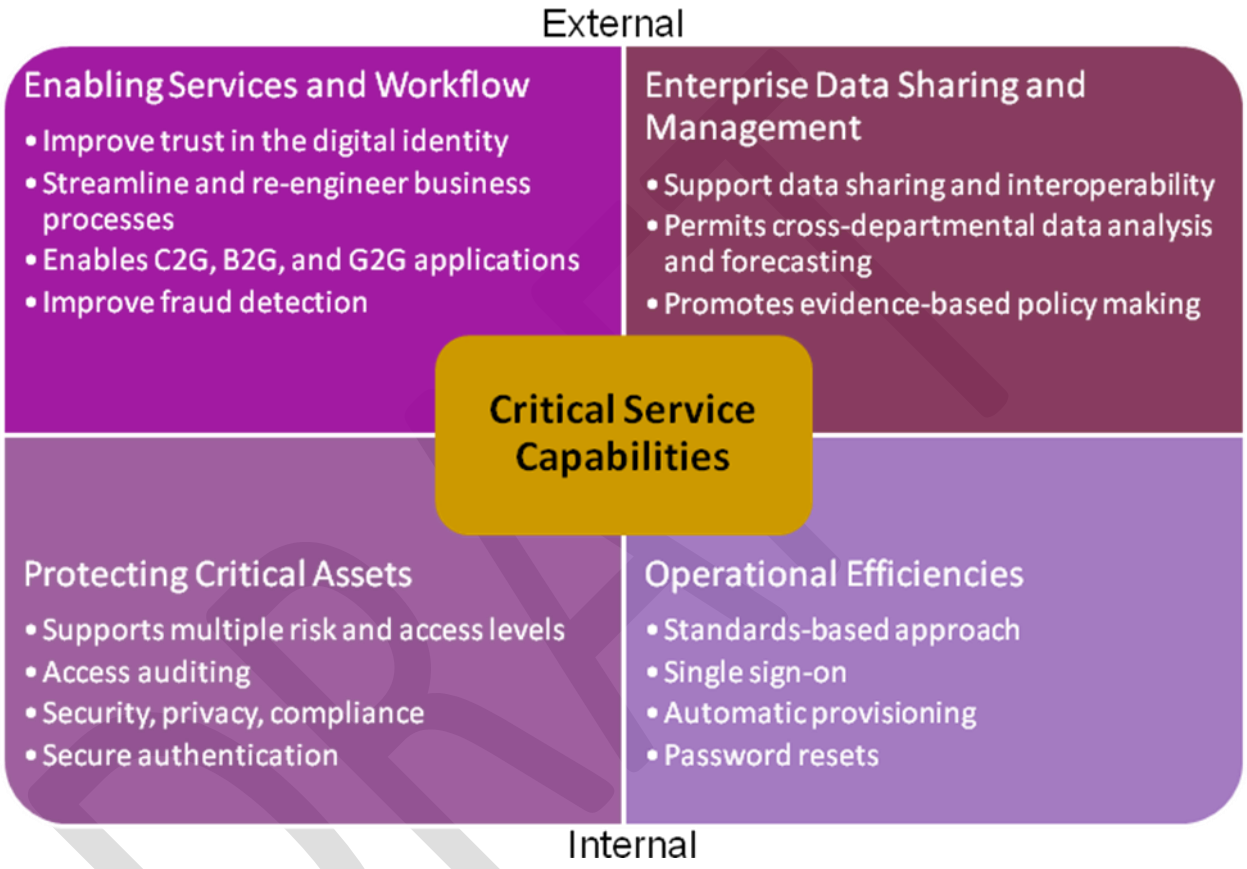
Proactive delivery of citizen services is also critical. Departments want to respond quickly to a change in a citizen's employment, legal or health status, and automatically deliver or remove the services the citizen is eligible for. This improves the well-being of the population and can help reduce the billions of dollars in services fraud the States experience today

The key to measuring the success of programs and delivering services to citizens proactively is the concept of a statewide unique identifier along with appropriate statewide, centralized identity services and federated identity management. In the case of SLDS, in order to link educational data from multiple departments and determine a correlation, there must be a common unique identifier for a student between these systems. Similarly in the case of delivering or removing citizen services, departments must communicate basic demographic information (e.g., name, address, dependent) between themselves so that if one department receives new information about a citizen, other departments do as well.

There is a need to standardize and unify within and across state boundaries. Towards this end, and for the purposes of centralizing identity and access management across State and its business partners, a new centralized State Identity Credentialing and Access Management (SICAM) system will be created. The SICAM will leverage concepts of a FTM which will allow existing and new resources to be rapidly integrated and securely accessed across boundaries. Electronic authentication of individuals can provide the base elements to allow for secure electronic transactions at varying assurance levels; and establishing trust for multiple purposes and multi-layered security. In addition to improving access control across agency boundaries, another challenge is addressing the need to conduct electronic business with the public using strong authentication mechanisms. SICAM can also provide more resources and assurance levels for an agency enterprise to determine the true identity of a public user. While programs specific to a particular State agency are not discussed within this document, it is envisioned that all State agency IAM programs within Government will align with a central SICAM framework and the central infrastructure that will integrate resources and identity mechanisms across agencies boundaries.

1.2 Value Proposition

The purpose of this document is to provide agencies with architecture guidance that addresses existing IAM concerns and how new systems must be designed to integrate within the SICAM Federated framework. This document provides guidance to agencies to gain significant benefits around security, cost, and interoperability thus providing positive impacts beyond an individual agency in improving delivery of services to the citizens of the State. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the Government and its business partners and constituents.



Identity and access management technologies are enabling, foundational tools supporting multiple business facets, both internal and external. The benefits associated with a centralized and federated implementation of IAM are summarized below:

Increased security, which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, IAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.
Compliance with laws, regulations, standards and state policies.
Improved interoperability, specifically between agencies using credentials along with other third party credentials that meet the requirements of the federated trust framework.
Enhanced customer service, Facilitating secure, unified, and user-friendly transactions – including information sharing – translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.

Elimination of redundancy, both through agency consolidation of processes and workflow and the provision of government-wide services to support IAM processes. This results in extensibility of the IT enterprise and reduction in the overall cost of security infrastructure.
Increase in protection of personally identifiable information (PII) by consolidating and securing identity data through the use of encryption, improving access controls, and automating provisioning processes.

The cybersecurity posture is improved through these benefits across the State Government with standardized controls around identity and access management. The IAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. This document presents a common framework and implementation guidance needed to plan and execute IAM programs. The Transition Roadmap and Milestones presented in Chapter ?? outlines several new agency initiatives and numerous supporting activities that agencies must complete in order to align with the government-wide SICAM framework.

1.3 Scope

Not all State electronic transactions require authentication; however, this guidance applies to all such transactions for which authentication is required, regardless of the constituency (e.g. individual user, business, or government entity).

- This guidance applies to remote authentication of human users of State agency IT systems for the purposes of conducting government business electronically (or e-government). Though that authentication typically involves a computer or other electronic device, this guidance does not apply to the authentication of servers, or other machines and network components.

- This guidance is intended to help agencies identify and analyze the risks associated with each step of the authentication process. The process includes (but is not limited to) identity proofing, credentialing, technical and administrative management, record keeping, auditing, and use of the credential. Each step of the process influences the technology's overall conformance to the desired assurance level.

- This guidance does not directly apply to authorization. Authorization focuses on the actions permitted of an identity after authentication has taken place. Decisions concerning authorization are and should remain the purview of the business process owner.

- This guidance does not address issues associated with "intent to sign," or agency use of authentication credentials as electronic signatures. For more information on electronic signatures, see the OMB guidance on implementing GPEA1 and the Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-2292.

There are two types of individual authentication:

a) Identity authentication—confirming a person's unique identity.

b) Attribute authentication—confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).

Attribute authentication is the process of establishing an understood level of confidence that an individual possesses a specific attribute. If the attribute does not provide ties to the user's identity; it would be considered an anonymous credential (discussed further in Section 4.2). Attribute authentication is not specifically addressed in this document; however agencies may accept 'anonymous credentials' in certain contexts.

1.4 Document Overview

The SICAM provides a blueprint for a statewide identity management solution. The document starts off by providing a background information and sites value proposition statements followed by framing this documents scope. The following briefly describes the sections and content contained within each section.

Section 1: The goals and objectives primarily focus on the role of the State Government in achieving the SICAM end-state, other key stakeholders have a crucial role in enabling interoperability and trust across the SICAM landscape to accomplish secure information sharing outside of State Government boundaries. Stakeholders, mentioned throughout this document, include external business and commercial entities wishing to conduct business with State Government; the health IT community as it increases its reliance on SICAM activities in order to facilitate the use of e-health records; Federal/Emergency Response Official (F/ERO) – emergency preparedness; and federal, local, and tribal governments that require information exchanges to meet mission needs.

2. Goals and Objectives: The Identity, Credential and Access Management Maturity Model identifies the goals and objectives to be met over the lifecycle of an IdAM presence across the enterprise. The maturity model represents a flexible and adaptive approach toward identification of the current IdAM presence and the next steps to be considered in advancing the maturity level of the IdAM solution.

3. Maturity Model: The Identity, Credential and Access Management Maturity Model identifies the goals and objectives to be met over the lifecycle of an IdAM presence across the enterprise. The maturity model represents a flexible and adaptive approach toward identification of the current IdAM presence and the next steps to be considered in advancing the maturity level of the IdAM solution.

4. Architecture Framework: Development of the SICAM Architecture Framework provides the rules and definitions necessary for the integration of information and services at the design level. The framework combines business and environment processes and represents the blueprint for the implementation of the IdAM solution. The blueprint contains the details that are essential for allowing data to flow from agency to agency.

5. Implementation Strategy: The federated identity management reference architecture outlines the target framework that the SICAM must fit within. This section will also outline how interoperability will occur to share identity attributes across agency boundaries in an effort to

reduce the total cost of ownership for agency identity systems and to improve the identity assurance levels for agencies that leverage these services.

6. Use Cases: In this section we introduce several hypothetical use cases and show how they might be able to take advantage of identity federation to improve customer experiences and reduce cost and improve overall security. The use cases section describes a typical enterprise topology and then describes uses cases followed by the details of those use cases.

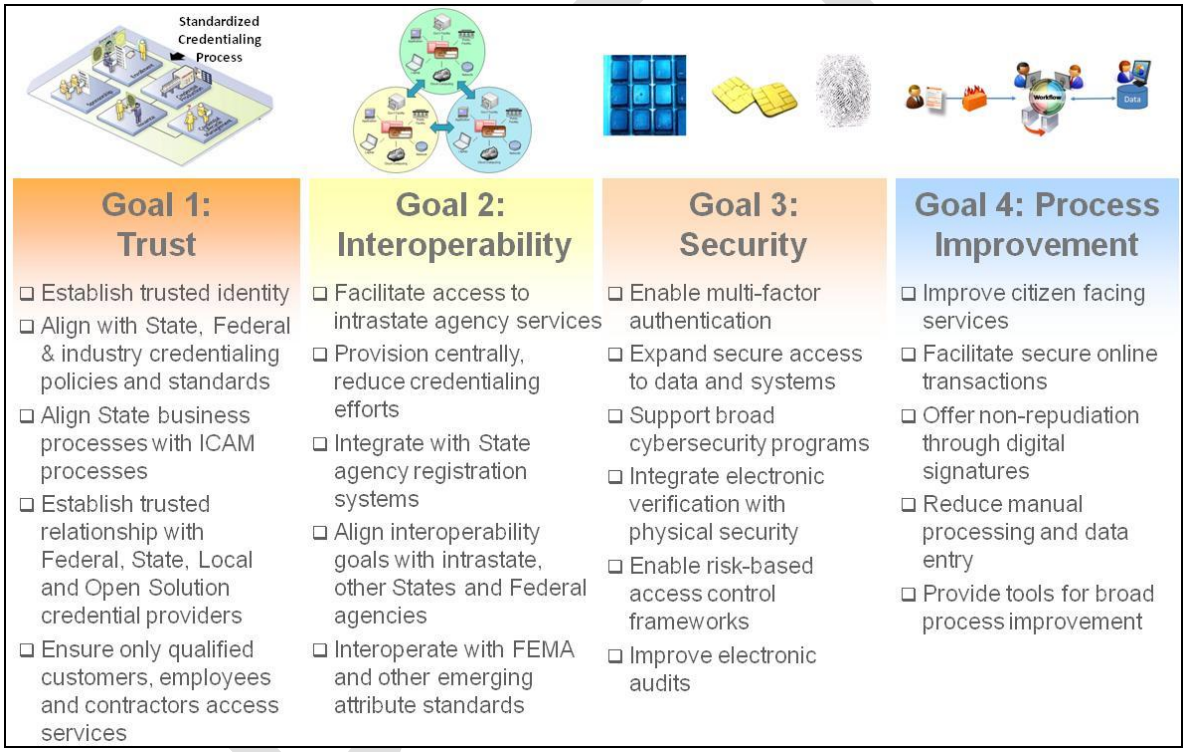
7. Summary: There are many steps along the way and an organization may find that not all of the areas fit neatly within the lines. Maturity within the architecture framework will vary across the business architecture processes, technology architecture, as well as the architecture blueprint. This is an ever-evolving process in the life of all organizations that leads to an efficient, effective responsive development and support organization for Identity and Access Management Solutions.

Appendix: Any addition to the document that can be used as reference material to further topics found within SICAM.

2. GOALS AND OBJECTIVES

The goals and objectives primarily focus on the role of the State Government in achieving the SICAM end-state, other key stakeholders have a crucial role in enabling interoperability and trust across the SICAM landscape to accomplish secure information sharing outside of State Government boundaries. Stakeholders, mentioned throughout this document, include external business and commercial entities wishing to conduct business with State Government; the health IT community as it increases its reliance on SICAM activities in order to facilitate the use of e-health records; Federal/Emergency Response Official (F/ERO) – emergency preparedness; and federal, local, and tribal governments that require information exchanges to meet mission needs.

The primary SICAM goals and objectives are organized into the following four categories:



2.1 Goal 1: Trust

States have traditionally played an active role in establishing and maintaining the identity of their constituents. The issuance of birth certificates, public school identification cards and driver's licenses are examples of instances where identities are established and credentials are issued at the state and local level. The challenge across states is that there are wide variances in the policies, practices and standards followed to establish identities. It is because of this variance that universal trust of identities and credentials across states and municipalities has not occurred.

State Government stands to gain great value and enhanced service delivery by developing a foundation of inter-organizational trust and interoperability across the State enterprise. Strong interoperable State identity credentials are the key to streamlining and automating building access, temporary access requests, and other access and authorization for government purposes. State Government must tackle the governance and technical challenges posed by the abundance, variety, and complexity of CA-ICAM-related programs in order to promote trust and interoperability and enable service delivery and information sharing across all partners.

Goal 1 is focused on establishing common standards, policies and practices for identity verification and vetting and credential issuance. With common, auditable identity and credentialing standards, all states will eventually be able to trust the identity of individuals presenting another states' credential.

Objective 1.1: Align with State, Federal and Industry Credentialing Standards, Policies and Processes

For the past several years there have been many inter-related but distinct State / Federal government and Industry initiatives to establish standard frameworks for Identity, Credentialing and Access Management. In addition, programs within other communities of interest have begun identifying their own identity, credential, and access management requirements, needs and procedures. States should leverage the existing knowledge bases, guidance and best practices which include:

Industry Bridges such as SAFE BioPharma1 and Transglobal Secure Collaboration Program (TSCP)2

Federal Guidelines including Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance3, Homeland Security Presidential Directive 12 (HSPD-12)4 and Federal Information Processing Standard 201 (FIPS 201)5 and associated Special Publications 6

Objective 1.2: Establish Trusted Relationships with State, Federal, Local and Standards-Based Open Credential Providers

By establishing trusted relationships with other State, Federal and open credential providers, states can avoid the requirement to independently credential all its citizens. It can instead become a relying party of other identity credentials by establishing policies to accept credentials it deems trustworthy. Trusted physical and logical credentials and standards may include:

Federal Personal Identity and Verification (PIV), PIV Interoperable (PIV-I) and First Responder Authentication Credentials (FRAC)

Kantara Initiative7 and InCommon Federation8 digital identity standards

[1] http://www.safe-biopharma.org/

[2] http://www.tscp.org/

[3] http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

[4] http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

[5] http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[6] NIST Special Publications 800-37, 800-53, 800-63, 800-73, 800-76, 800-78 – http://csrc.nist.gov/publications/PubsFIPS.html

[7] http://kantarainitiative.org/

[8] http://www.incommonfederation.org/

Objective 1.3: Comply with State Laws, Regulations, Standards, and IAM Governance
This objective includes aligning and coordinating operations and policies to meet the laws, regulations, standards, and other guidance in forming IAM systems; aligning State agencies around common IAM practices; and where necessary, reviewing and aligning policies to ensure consistency.

Objective 1.4: Establish and Enforce Accountability for IAM Implementation to Governance Bodies
Necessary authority must be given to and exercised by the SICAM governance authorities (outlined in Section 2.3.1) to ensure accountability across State Government in meeting its IAM vision and in alignment with Executive Order S-03-10. In addition to developing comprehensive guidance and standards in support of the SICAM segment architecture, the governance bodies must establish and track specific performance metrics. Each agency shares the responsibility for establishing the trust and interoperability processes necessary to achieve the IAM vision / end state and may be asked to report status against performance metrics periodically to a governing body.

Objective 1.5: Promote Public Confidence through Transparent IAM Practices
Public confidence in the security of the state government's electronic information and information technology is essential to adoption and use of E-Government services. State Government must build a robust framework of policies and procedures committed to respecting and protecting the privacy of users in order to enable the trust required to move State Government transactions online.

Objective 1.6: Establish and Maintain Secure Trust Relationships
Establishing compatible identity, credential and access management policies and approaches and a framework for evaluating partners against these policies is a critical success factor in building trust relationships across the health care, government, commercial, and state enterprises. State agencies will identify and leverage existing trust relationships and continue working to build new trust relationships within the government enterprise and between the Government and its partners (other governments, businesses, the health care community, and the State public) in order to move transactions online.

2.2 Goal 2: Interoperability

States and municipalities have been issuing a multitude of single-use credentials to their constituents over the years. While these library, recreation center, Medicaid, Medicare, Drivers, Fishing, employee IDs/Licenses serve their purpose to provide authorization to use a particular facility or service – they redundantly attempt to establish identity and at varying levels of trust and including differing tamper proof features. The goal of interoperability is to establish common credentials – both physical and logical – that can be used to uniformly establish identity and that can be used to provide authorizations across facilities and services.

A key objective of the SICAM segment architecture is to implement a holistic approach for State Government-Wide identity, credential and access management initiatives that support access to State IT systems and facilities. By the end of FY 2012, it is intended that all State agencies will implement and/or provide a coordinated approach to SICAM across E-Government interactions

[Government-to-Government, Government-to-Business, Government-to-Citizen, and Internal Effectiveness and Efficiency (IEE)] at all levels of assurance as defined in Section x.x.

The SICAM segment architecture also provides a framework that may be leveraged by other identity management architectural activities within specific communities of interest. The aim is a standards-based approach for all State government-wide identity, credential and access management to ensure alignment, clarity, and interoperability.

Objective 2.1: Support Information Sharing Environment (ISE) Communities of Interest
State Government operations rely on collaboration and knowledge sharing with other communities (to include Health IT, federal/local/tribal governments, industry, and foreign governments) in order to conduct business. This information sharing demands trust among the various players and an IAM capability which supports this scope of interoperation. Future federation solutions must acknowledge and account for the need to support interoperable access to systems and data to support information sharing while maintaining control of the allowed access and appropriate information protections. The SICAM segment architecture addresses the concept of federated information flow, which requires two or more federated enterprises to support transactions across common interfaces.

Objective 2.2: Align Processes with External Partners
The SICAM segment architecture supports a consistent approach for all government-wide identity, credential and access management processes to ensure alignment, transparency, and interoperability. This allows State Government a means to do business with organizations such as banks and health organizations and support G2B transactions by enabling common standards and leveraging an existing federated infrastructure. State Government will respect the different requirements of state agency partners as to risk, assurance, and mission, and provide solutions that meet those needs and maintain inter-agency and inter-organizational interoperability.

Objective 2.3: Leverage Standards and Commercial Off-the-Shelf Technologies for IAM Services
State Government agencies will use commercial off the shelf (COTS) products and services, whenever possible, in order to enhance interoperability with the use of open standards and protocols and technological innovation and promote availability of SICAM systems and components.

Objective 2.4: Increase Interoperability and Reuse of IAM Programs and Systems
Implementation of the IAM segment architecture is intended to unify existing IAM programs and initiatives, as well as agency-specific IAM activities, under a common governance framework, recognizing the unique role of each program in the overall structure while eliminating redundancies and increasing interoperability between solutions.

2.3 Goal 3: Security (Improve Security Posture across the State Enterprise)

ICAM capabilities play a key role in enhancing the ability to prevent unauthorized access to State Government systems, resources, information, and facilities. As a function of logical security, IAM can help protect information's confidentiality, assure that the information is not altered in

an unauthorized way, and ensure information is released only to those entities authorized to receive it. IAM will support and augment existing security controls as specified by the Federal Information Security Management Act (FISMA) and supporting NIST Special Publications 800-53 and 800-37, by promoting the use of strong identity solutions appropriate to the environment. A focus on IAM outcomes—who has access to data and resources, what information is collected—can help improve security posture beyond what controls are in place to meet mandates.

Objective 3.1: Enable Cyber Security Programs
ICAM is a critical piece in protecting information and achieving cyber security goals. As a rising priority, cyber security will continue to grow and change within State Government. Collaboration and coordination between IAM and cyber security governance led by the OCIO is a critical success factor.

Objective 3.2: Integrate Electronic Verification Procedures with Physical Security Systems
Once IAM systems are in place and well established, the next step is for agencies to establish the need for electronic physical security systems and adopt and implement the appropriate policies and technologies to support physical access control leveraging electronic authentication.

Objective 3.3: Drive the Use of a Common Risk Management Framework for Access Control Mechanisms
Existing authentication guidance and best practices for both logical and physical access dictate the use of a common risk management approach in determining the appropriate credential types and access control mechanisms. The OCIO will work to drive the adoption and use of these approaches to ensure access controls are compliant with security requirements and risk-based analyses.

Objective 3.4: Improve Electronic Audit Capabilities
Solutions adopted as part of SICAM initiatives will provide robust auditing capabilities to support accountability, provide discrete non-repudiation, and enhance transparency in security effectiveness.

2.4 Goal 4: Process Improvement (Facilitate E-Government by Streamlining Access to Services)

Strong and reliable identity, credential, and access management is a key component of successful E-Government implementation. When enabling electronic government, programs share sensitive information within government, between the government and private industry or individuals, and among governments using network resources and the World Wide Web. Further, this move towards enabling E-Government must be achieved in a flexible, cost-effective manner through collaboration among the public, industry, academia, and the government; and a corresponding policy and management structure must support the implementation of the solution.

Another goals of this effort is to allow agencies to create (and maintain) information systems that deliver more convenience, appropriate security, and privacy protection more effectively

and at a lower cost. Establishing a clear vision is the first step in supporting these goals. Below are some specific benefits that may be realized from implementing this vision.

Objective 4.1: Expand Secure Electronic Access to Government Data and Systems
To align with the SICAM segment architecture, state agencies should design, build, and deploy IAM solutions to support a broad range of electronic government use cases which will support their mission areas across Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C) interactions. State agencies must cooperate across agency boundaries in service delivery to give citizens, businesses, and other governments increased electronic accessibility to State Government services through a wide choice of access mechanisms. The implementation of SICAM initiatives will facilitate the creation of government services that are more accessible, efficient, and easy to use.

Objective 4.2: Reduce Administrative Burden Associated with Performing IAM Tasks
Current IAM efforts still rely on numerous manual, paper-based processes. Through automation and streamlining processes, State Government stands to significantly reduce the administrative burden and cost associated with the various IAM tasks. For instance, the legacy practice of manually administering user accounts/privileges on a system-by-system, user-by-user basis creates a great administrative burden.

Objective 4.3: Align Existing and Reduce Redundant IAM Programs
A key objective of the SICAM segment architecture is to reduce or eliminate duplicative efforts and stove-piped programs and systems related to identity vetting, credentialing, and access control. Future IAM solutions will leverage the existing investments of the central SICAM system and provide a more efficient use of tax dollars when designing, deploying and operating IAM systems.

2.5 How to the Goals and Objectives Should be Used

By aligning the goals with objectives we illustrate how to identify the concepts that need to be addressed in order to provide a Federated IdAM solution. The objectives serve as a roadmap for businesses to analyze what needs to be done to meet the value propositions of providing a centralized federated IdAM.

3. SICAM MATURITY MODEL

The Identity, Credential and Access Management Maturity Model identify the goals and objectives to be met over the lifecycle of an IdAM presence across the enterprise. The maturity model represents a flexible and adaptive approach toward identification of the current IdAM presence and the next steps to be considered in advancing the maturity level of the IdAM solution.

The SICAM Maturity Model provides a path for architecture and procedural improvements within an organization. As the architecture matures, predictability, process controls and effectiveness also increase.

Whatever the current stage of the organization's IdAM program, each activity undertaken also has its own lifecycle. Without continuous monitoring of the driving business and technology factors, any IdAM Framework Architecture can soon become obsolete. Just as individual product and compliance components need to go through the cyclic process of Documentation, Review, Compliance, Communication, and Vitality, the high-level IdAM Architecture Framework and procedures must be reviewed and updated to properly reflect environmental changes.

Maturity Levels	Trust	Interoperability	Security	Process Improvement	
Level 1	Issuing Level 1 Credential	Single Agency Issuing Level 1 Credential	Minimal to No Verification of Identity, Basic Credential	Minimal Efficiency Gains through Centralized Issuance	Identity / Credential
	Accepting Level 1 Credential	Single Agency Use of Level 1 Credential for Physical Access	Physical Access Control with Self-Asserted Credential	Minimal Physical Access Efficiency Gains	Access Management
Level 2	Issuing Level 2 Credential	Single Agency Issuing Level 2 Credential	Strong Verification of Identity, Basic Credential	Minimal Efficiency Gains through Centralized Issuance	Identity / Credential
	Accepting Level 2 Credential	Multiple Agency Use of Level 2 Credential for Physical Access	Physical Access Control with Level 2 Credential	Standardized Physical Access Controls	Access Management
Level 3	Issuing Level 2 / 3 Credential and Digital Identity	Multiple Internal Points of Issuance	Strong Verification and Binding of Identity	Reduced Emphasis Central Issuance	Identity / Credential
	Accepting Level 2 / 3 Credential and Digital Identity	Multiple Agency Use of Credential and Digital Identity	Physical and Logical Access Control	Standardized Physical and Logical Access Controls	Access Management
Level 4	Issuing Level 4 Credential	Multiple Internal and External Points of Issuance	Highest Level of Verification and Binding	Widespread Issuance Reduces Internal Issuance Needs	Identity / Credential
	Accepting Level 4 Credential	Multiple Cross-Agency, Cross-State Use	Risk Based Physical and Logical Access Controls	Achieving Business Process Improvements	Access Management

The Identity, Credential and Access Management Maturity Model envision a continuous improvement process, migrating from Level 1 through Level 4. The diagram above summarizes the Identity / Credential and Access Management maturity levels across the 4 main SICAM goals.

Basically, the further you go down the stack in levels of maturity the more mature your total solution for IdAM becomes. Trust, Interoperability, Security, and Process Improvement goals become realized as we move from Level 1 through 4.

3.1 Level 1

Identity credential with user name and passwords to a risk based interoperable identity credential commensurate with the level of facility, network, application or data being accessed. Issuing interoperable Level 3 identity credentials with verified names, soft crypto token or one time password device matures identity credential systems.

3.2 Level 2

Identity credential with user name and passwords to a risk based interoperable identity credential commensurate with the level of facility, network, application or data being accessed. Issuing interoperable Level 3 identity credentials with verified names, soft crypto token or one time password device matures identity credential systems.

3.3 Level 3

Identity credentials become more prevalent access management systems will mature by trusting or becoming a relying party of the credentials issued by another organization or state.

3.4 Level 4

PIV-I or other Level 4 interoperable hardware tokens optimizes maturity of a States identity credential program. Access management system maturity is optimized by relying on interoperable Level 4, 3, 2 and 1 credentials issued by other issuers commensurate with the level of risk of the facility, network, application or data being accessed.

3.5 How to use the SICAM Maturity Model

The SICAM Maturity Model can best be used to serve as a starting point for organizations who wish to participate either as a service provider (Node) or an organization who wishes to incrementally improve their IdAM posture by participating in an enterprise solution. In order to do this an organization would use the SICAM Maturity Model as a guideline in assessing their current status and define where they need to be. Some organizations will require only a level one maturity while others may even need to extend the maturity model for specific needs.

SICAM ARCHITECTURE CONCEPTS

This section introduces key principles and concepts which characterize SICAM architecture. Later sections of the document will discuss these principles and concepts in further detail and how they are applied within the architecture of SICAM.

3.6 Federated Approach

At its most fundamental level the SICAM architecture describes a centralized service based on a collection of data sources (or nodes) networked together and used for identification purposes. Networks may be modeled as graphs of nodes and the links between them. In the context of SICAM, a node is a entity that participates with other nodes in a central system that orchestrates the exchange of information for purposes of providing a level of assurance that the identity is who they say they are.

Regardless of its internal structure, an implementation of a centralized, federated architecture enables each node to maintain autonomy inside their domain, while adhering to SICAM specification for inter-node communication. This flexibility is achieved by the set or architectural principles, described in section 4.2 Architecture Principles, which define the SICAM design.

3.7 Architecture Principles

1. **Centralization:** The SICAM architecture allows decentralized Nodes to participate in the presentation of a single entry point for authentication.
2. **Separation of Authentication from Authorization:** A founding principle is to separate authentication functionality from authorization functionality. SIDCAM scope shall not include authorization concepts.
3. **Local Autonomy** – Acknowledges that the decision to release information from on Node to another is a local decision, governed by Federal and State regulations and local policies and permissions. Given this principle, SICAM transactions must include enough information about the originating Node (requestor/sender depending on whether it is a push or pull transaction) for the target SICAM Node to make a decision about whether to participate in the information exchange.
4. **Local Accountability** - Each SICAM Node is accountable for the accuracy and truth of the information it provides to assist the decision making process, as embodied by the local autonomy principle.
5. **Adherence to standards:** The SICAM has taken the initiative to adopt a series of harmonized standards which have been developed by voluntary consensus standards bodies for exchange of identity information among all such entities and networks.
6. **Service-Oriented, Layered Architecture:** There is a common messaging, security and privacy foundation which supports the SICAM identity information exchange services.
    - **Cross-platform integration** - Messages are the “universal translators” between different platforms and languages and permit each system to work with their native data types.

- **Reliable communication** - Messages can use a “store-and-forward” style for delivery.
- **End-to-end security** - Messages can transfer the complete security context using a combination of headers and tokens which increases the ability to improve control over the *authentication* of the personal identity .

7. **Utilizes Web Services:** Web Services provide the basis for transport, discovery and exchange capabilities.
   - **Standard protocol:** Functionality is exposed via web services interfaces.
   - **Web service description**: This description is provided via an XML document called a Web Services Definition Language (WSDL) document.
   - **Finding web services:** The discovery capabilities are provided by a listing of web services implemented via the SIDCAM Web Services Registry.

8. Utilizes **public key infrastructure** as the basis for security.

4. SICAM ARCHITECTURE FRAMEWORK

Development of the SICAM Architecture Framework provides the rules and definitions necessary for the integration of information and services at the design level. The framework combines business and environment processes and represents the blueprint for the implementation of the IdAM solution. The blueprint contains the details that are essential for allowing data to flow from agency to agency.

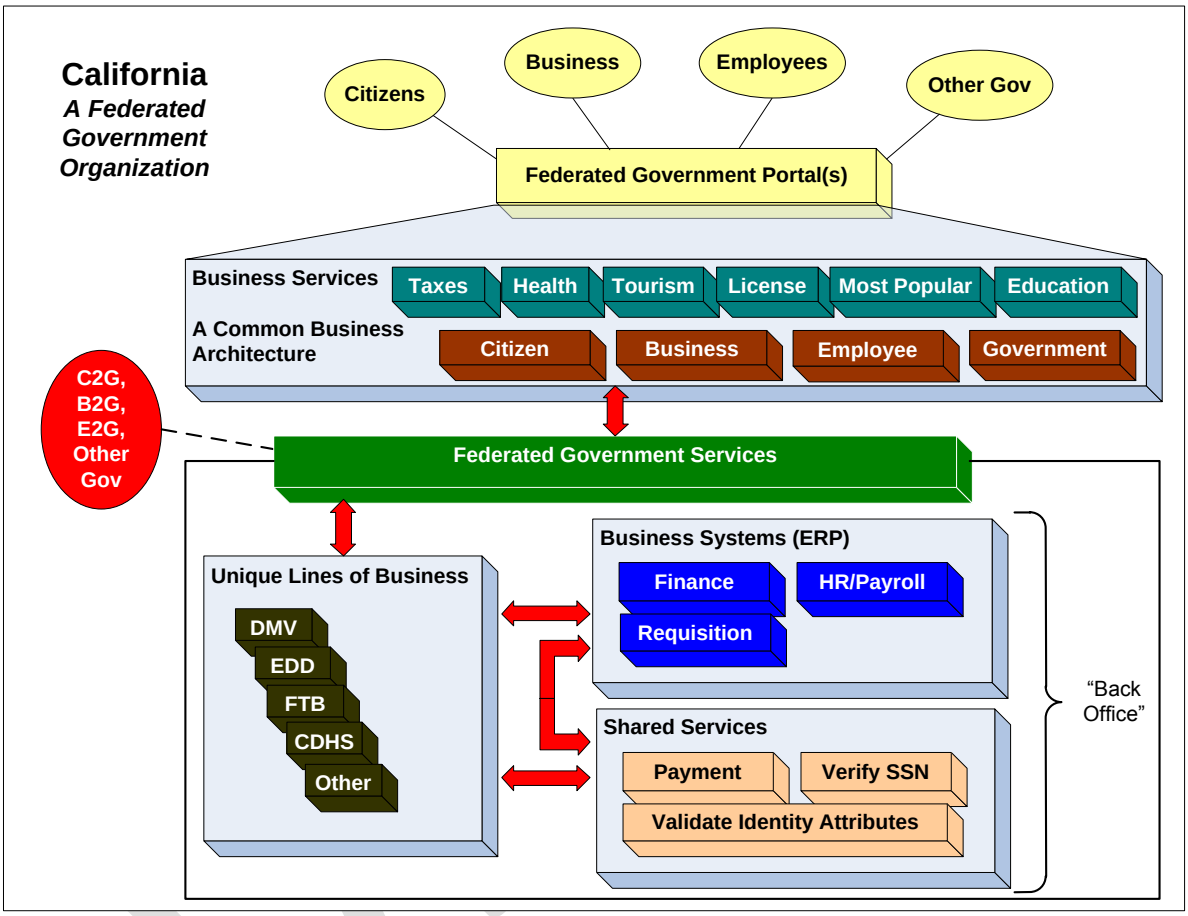
For agencies to become part of the SICAM federated framework, existing IdAM systems will need to address architectural elements to adapt and fit within the architectural framework of SICAM. Standards-Compliant deployment is critical and a key to success. After business issues are addressed, agencies must ensure that the technology being deployed is open and standards-compliant. The predominant standard for identity federation is the Security Assertion Markup Language (SAML), and the current version being 2.0. This protocol was developed through the input and extensive real-world experience of hundreds of major deployments and dozens of the leading vendors in the industry.

Identity federated as both a technology and business process can bring significant value to California's agencies and their business partners. It will provide the means of sharing necessary information between agencies and partners to increase identity assurance for business processes and the delivery of services to the public in a secure manner. SICAM can provide this opportunity without compromising the confidential information that is leveraged to increase that assurance.

The SICAM Architecture Framework focus for identity federation fits within a larger framework of sharing business services. In the context of identity federation, departments can offer a service that validates identity information. DMV for instance can validate citizen identity information and EDD can validate business entity information which may include employee information. The diagram (????) below illustrates this framework.

4.1 IdAM Architecture Framework Target

The architectural overview below illustrates a federated government framework that provides centralized services to citizens, business, employees, and other government entities that span state, local and federal jurisdictions. It illustrates how government entities can share services across independent information technology domains.

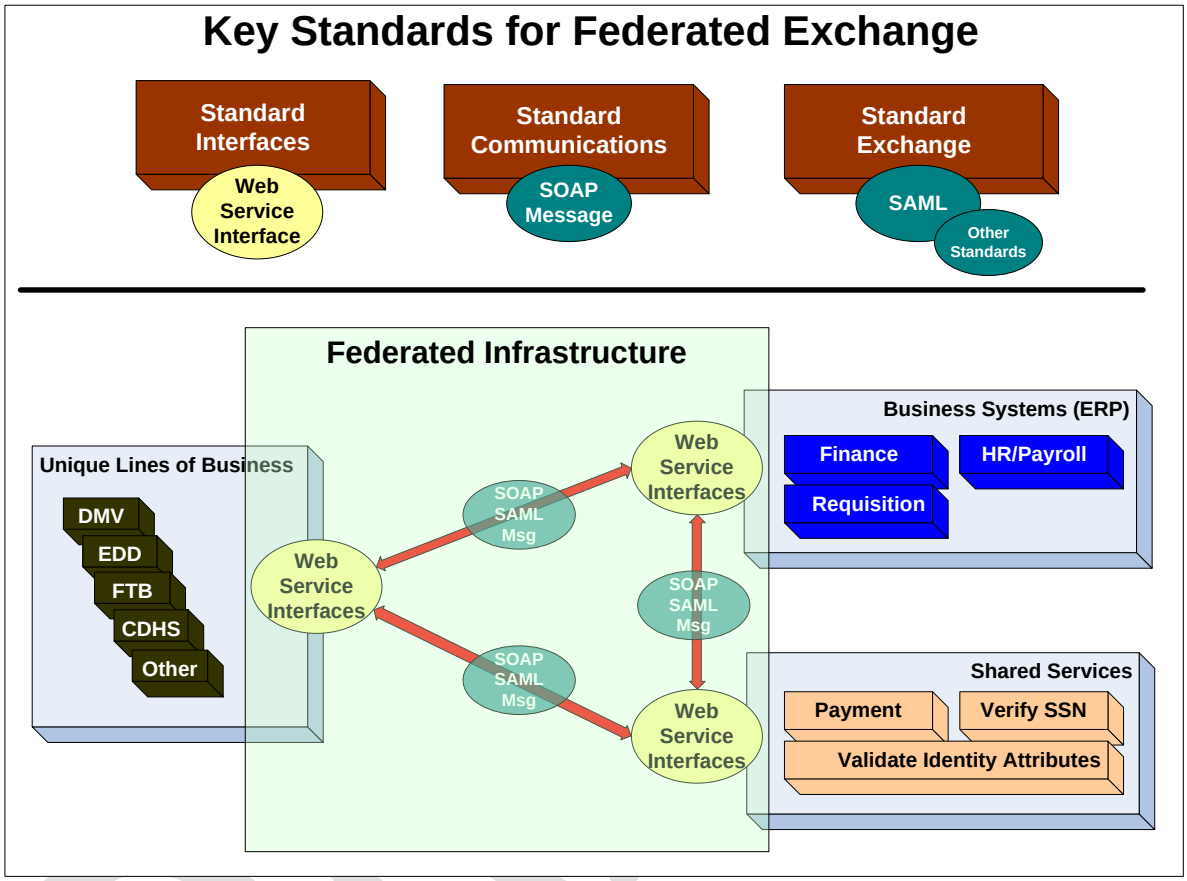


Stakeholders would have an opportunity to connect through portal web pages or interact through shared federated government services. Here is one scenario:

A citizen could connect through a state portal to obtain access to resources or benefits from a government entity. During this process, the citizen would be asked a series of questions to identify who they are. The questions may be based on credentials that the citizen holds that was issued to them from a government entity. The federated system would be used during this process to interact with other departments within the federated system. In this scenario, the federated system would provide identity validation before the citizen was granted access to the resources or benefits.

4.2 Key Standards for Federated Exchange

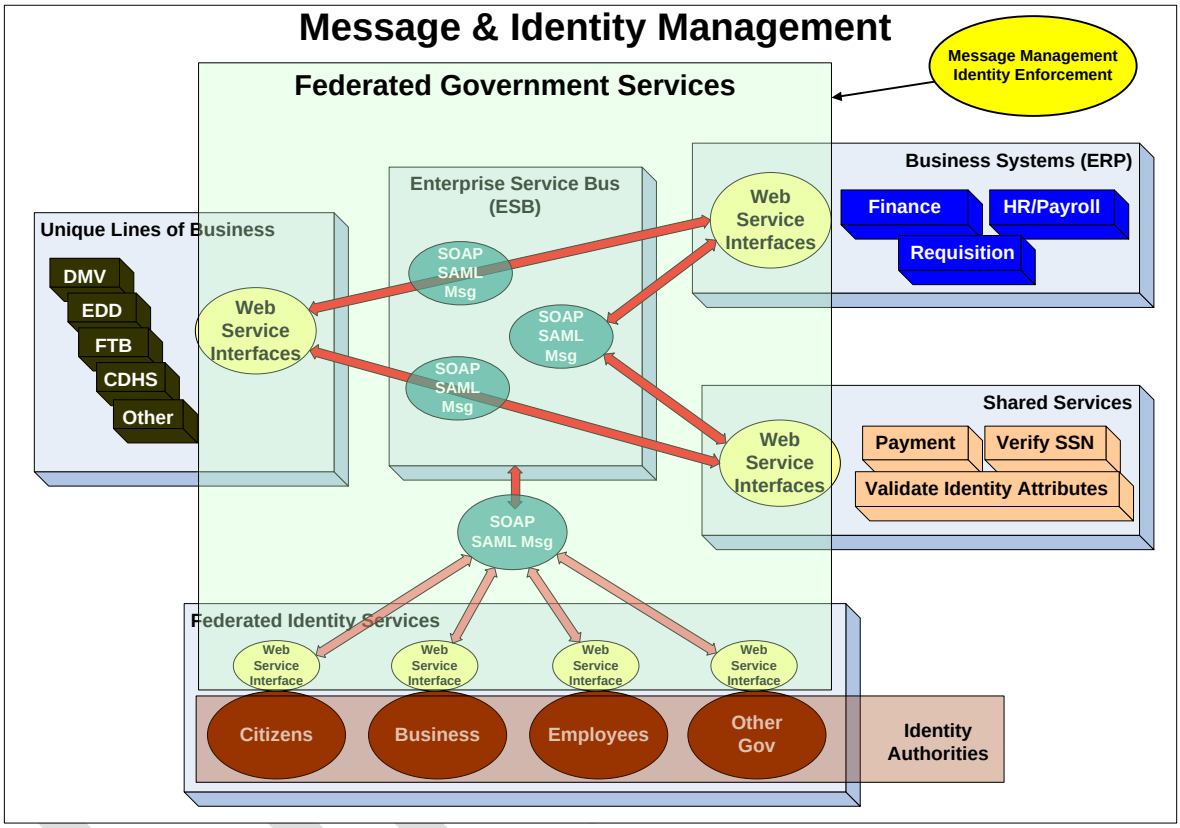
This diagram illustrates the key standards and how they interact in a federated services environment.



Standards such as Web Service for service interaction, the Simple Object Access Protocol (SOAP) for message format, and the Security Assertion Markup Language (SAML) for security exchange are established as the state standards for identity federation. This is critical for proper interaction and seamless integration for the federated organization.

4.3 Message and Identity Management

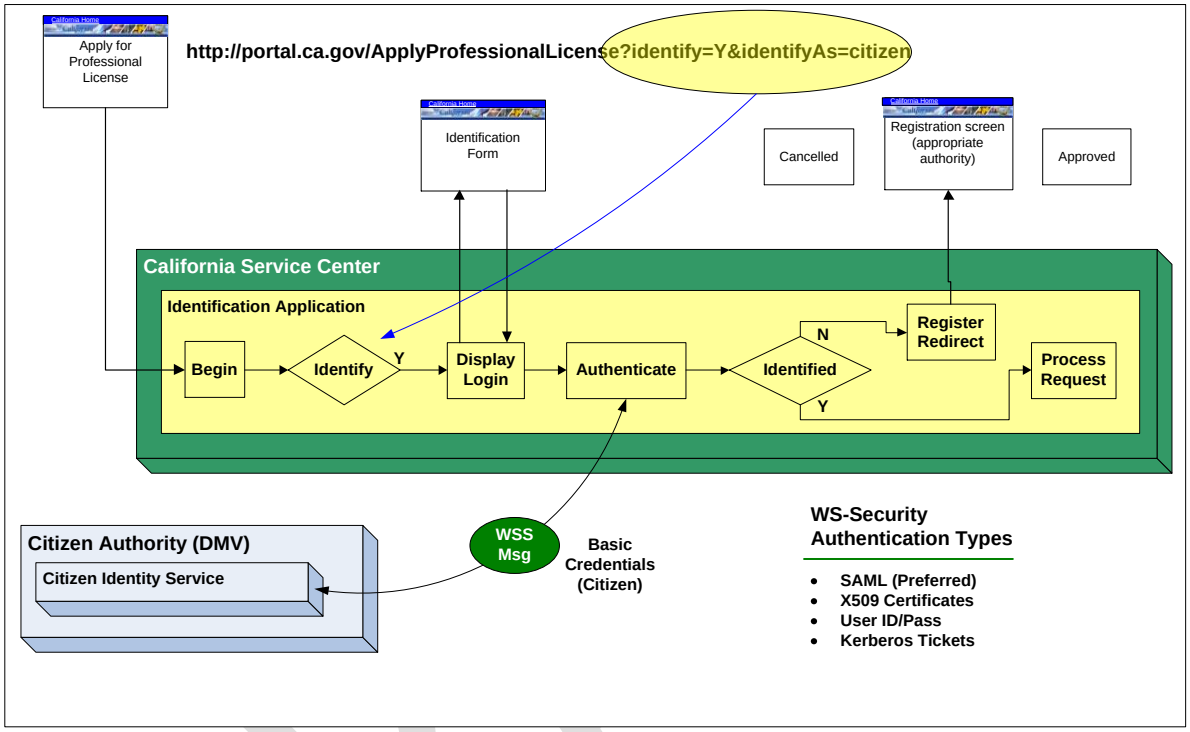
The primary focus and direction of the state is to leverage approved open standards for messaging and identity within the federated system. Since there will likely be a variety of disparate government systems interacting within the federated organization, this places even more importance on establishing acceptable use of open standards for messaging and identity.



The combination of service, message, and identity standards provides the opportunity to federate multiple governmental services. Infrastructure to support these standards will align with the size and cultural autonomy of the organization.

4.4 Authentication (Citizen Application for a License)

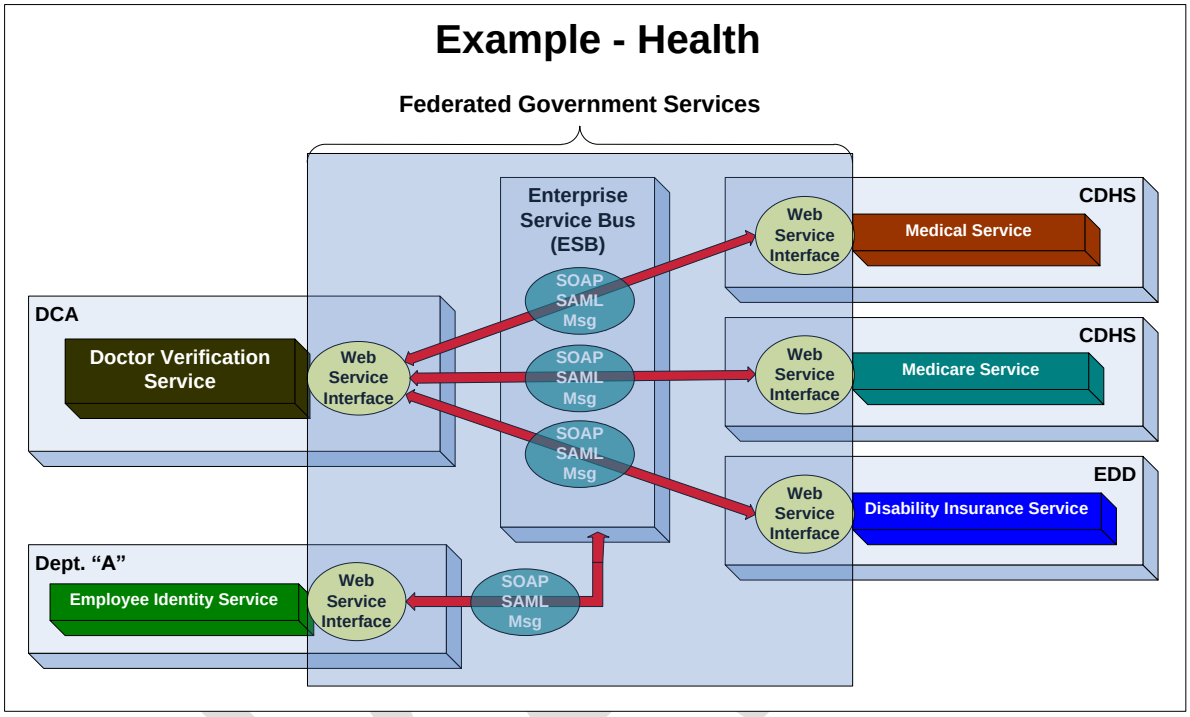
The diagram below illustrates specifics regarding the interaction between government services, messaging and identity authentication.



As shown above, the citizen is applying for a professional license through a state web portal. This is where the message flow behind the online screen begins and the identity of the citizen is authenticated through a citizen identity service. If there is a confirmed identity, the process flow continues which leads to the processing of the license. If an identity match does not occur, then a registration process is initiated that allows the citizen to validate and store their identity attributes in the citizen identity service.

4.5 Example: Health

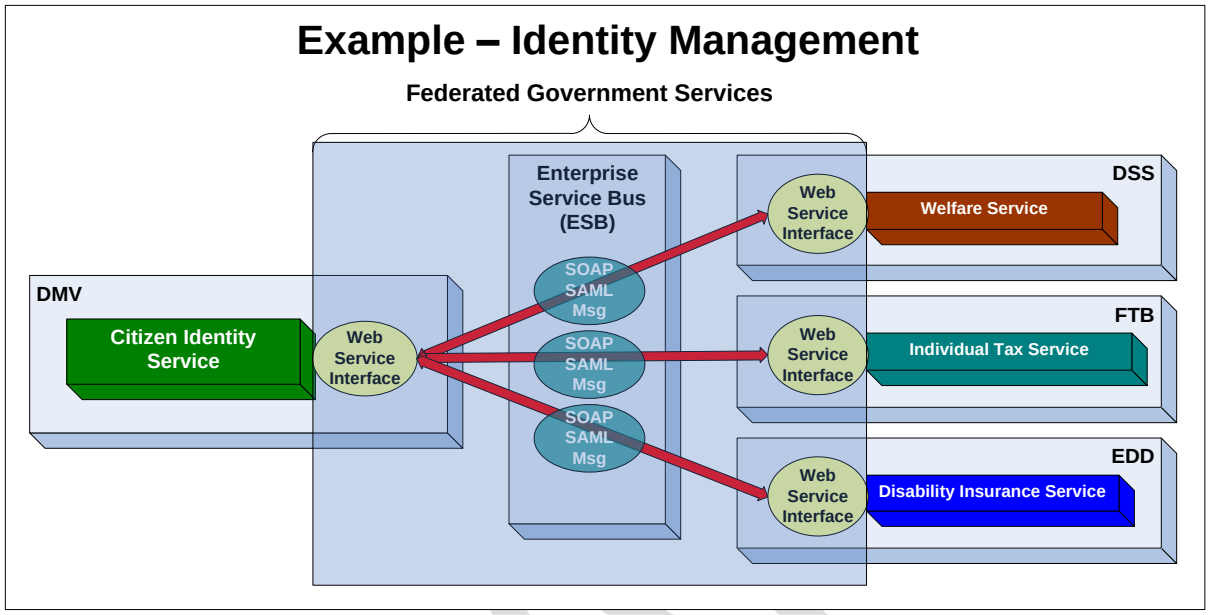
The diagram below illustrates how employees and physicians interact through the federated system utilizing open standards and a messaging and identity infrastructure.



This use case can be expanded to a Heath Information Exchange to support other social, health, and partner's needs.

4.6 Example: Identity Management

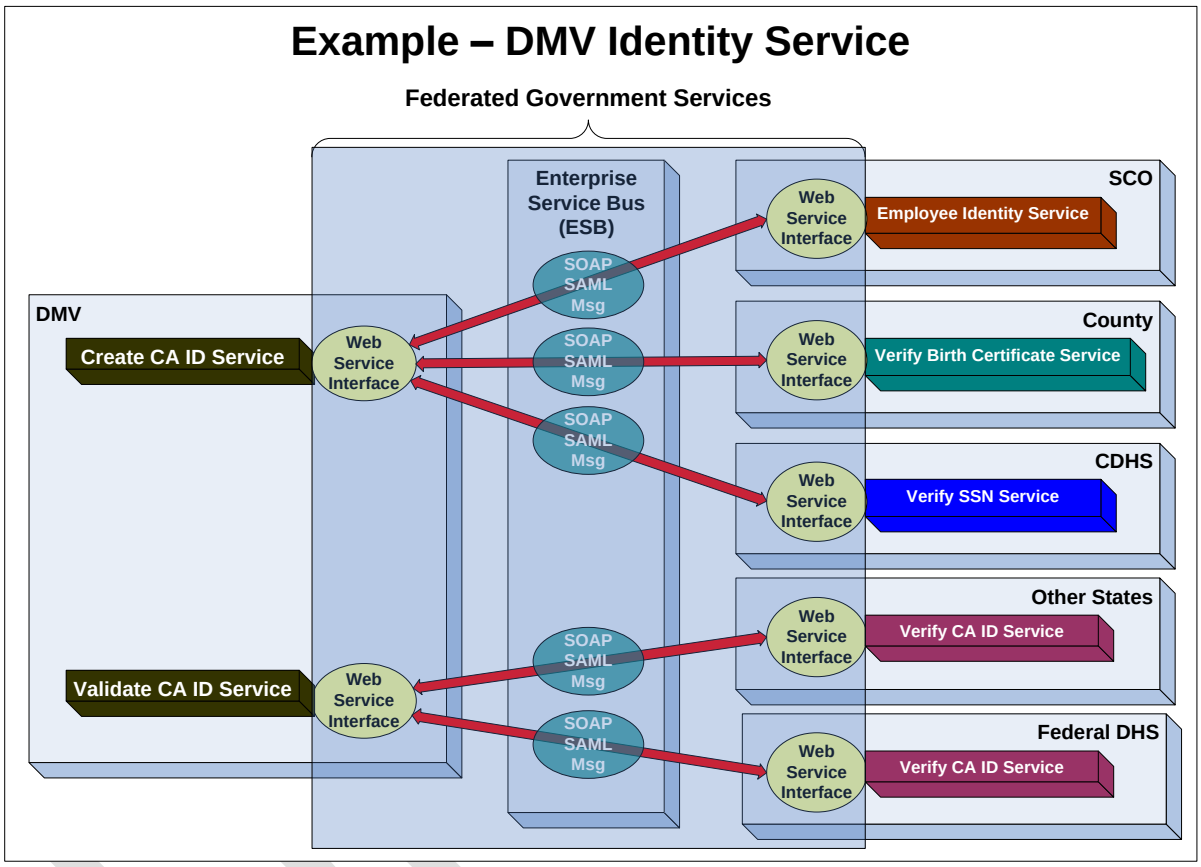
In the illustration below, the federated government system is used to validate Citizen Identity through a shared service provided by the Department of Motor Vehicles.



There are various navigation techniques that can guide the citizen through this process. They range from seamless to prompting the citizen to "ok" the validation using their DMV ID.

4.7 Example: Citizen Identity Service

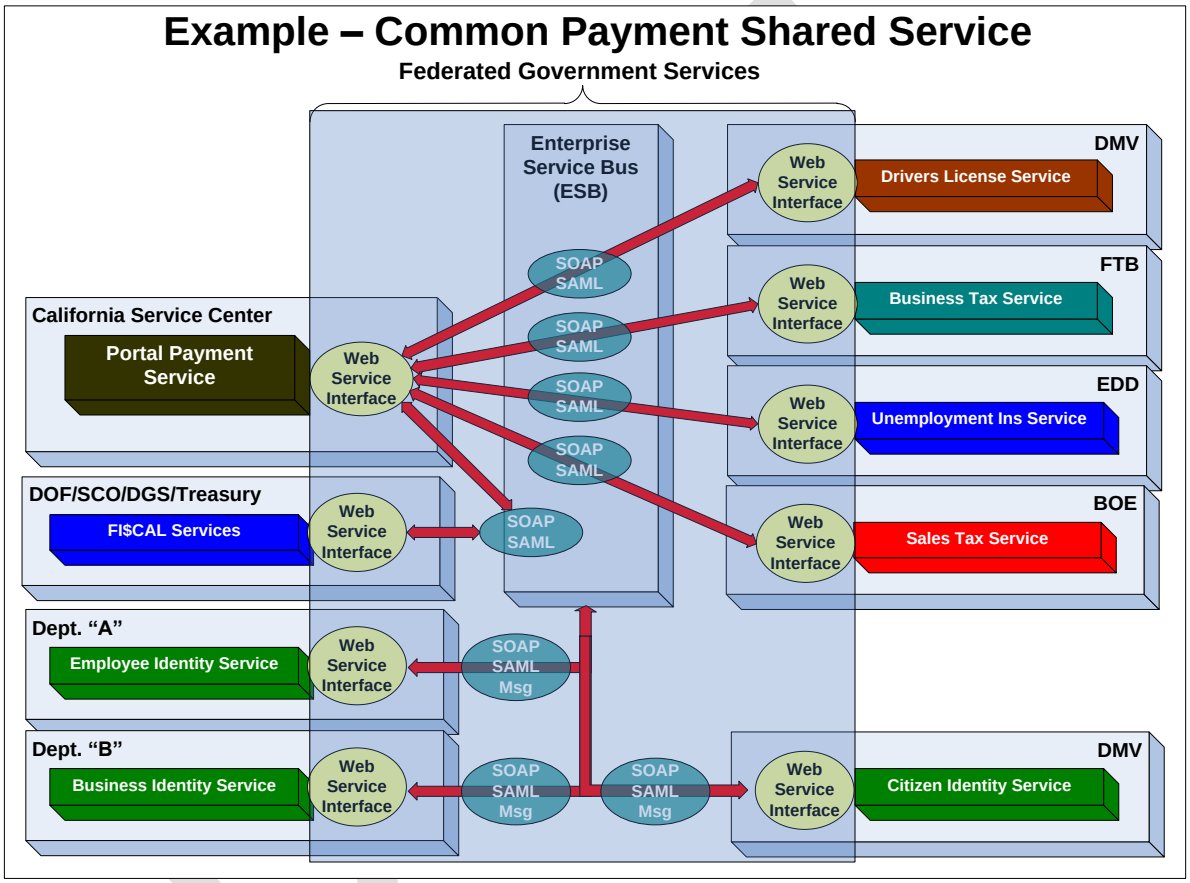
The illustration below shows how identity validation proofing can be performed once standards and infrastructure are in place. Interactions among the multiple governmental services provide real time proofing at time of identity registration.



As a part of the identity registration process being performed by the Department Of Motor Vehicles, the DMV validates information given to them by the citizen with other governmental services such as the County birth records, Department of Health Services, and the State Controllers office. Identity proofing is also validated through available federal services. This is not limited to government services only; private identity warehouses can all be included in the proofing process. The key is real time proofing while the citizen is physically present.

4.8 Example: Common Payment Shared Service

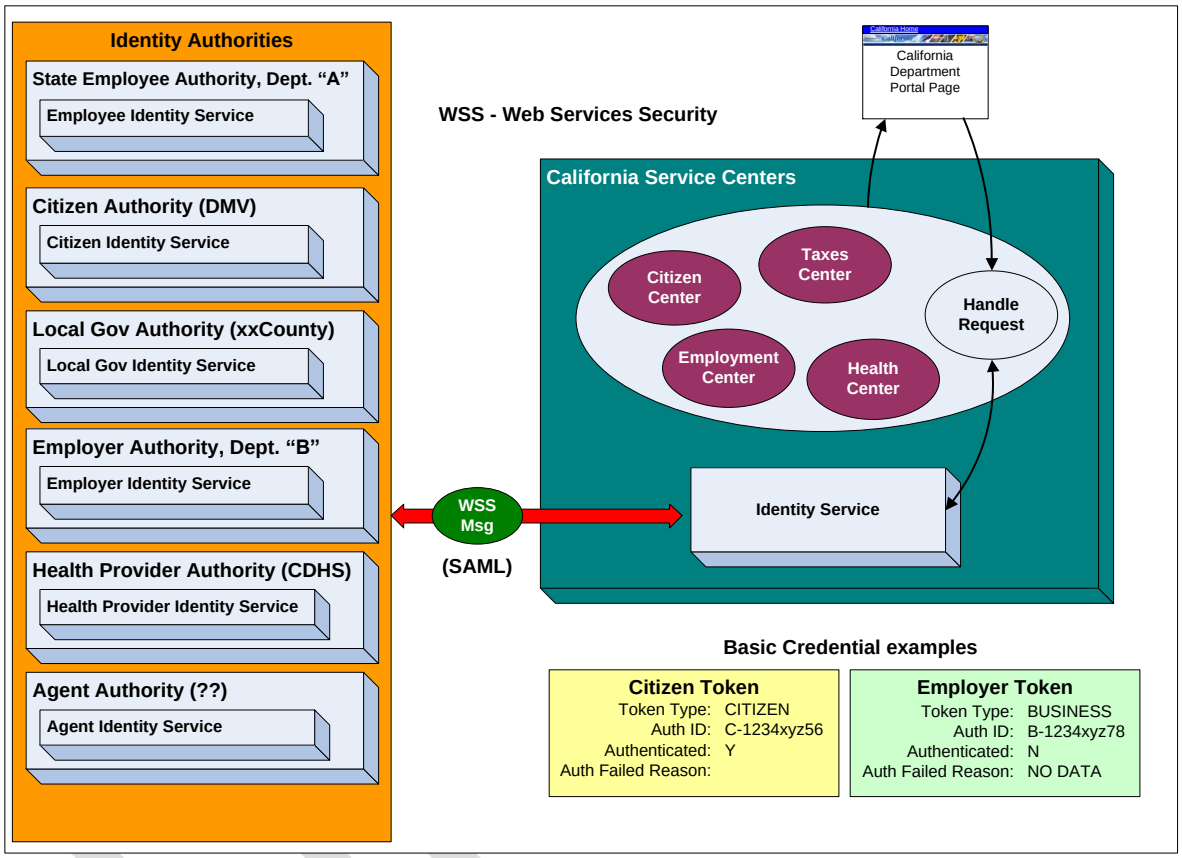
The illustration below shows how federated identity can provide the ability to implement more effective citizen interactions with government. In this example the Portal Payment Service provides a shopping cart experience for the citizen. They can make a single payment that will cover multiple liabilities to the State. The payment is properly allocated and posted by the representative department or agency and is processed by the State Treasury. Notification to other departments or agencies with the federation is easily facilitated.



The use of available technologies greatly enhances the federation of government services by inserting a level of abstraction among the different services. This allows only authorized messages to reach a specific service and allows for autonomy among the departments and agencies.

4.9 Identity Roles and Attributes

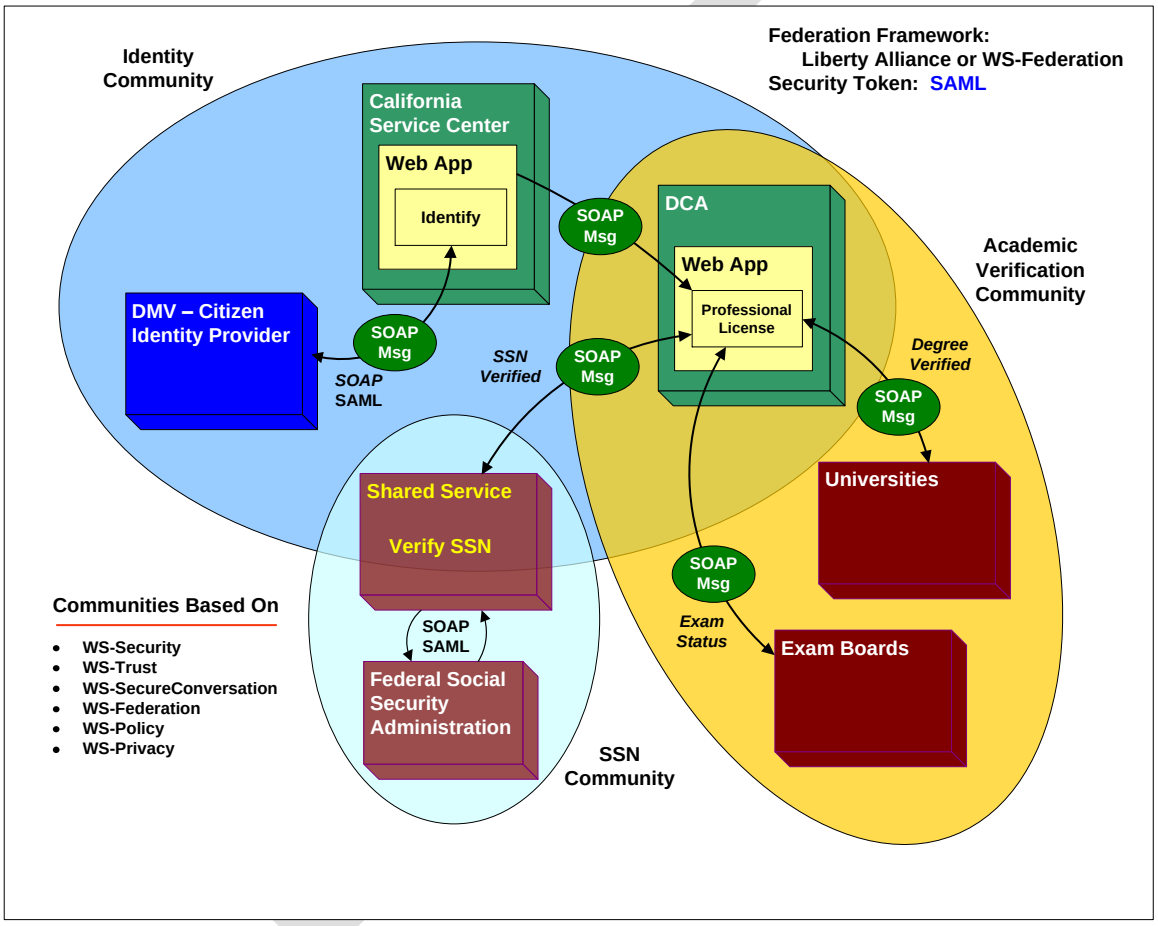
In a federated environment, a single entity or individual can have multiple roles. Role based security concepts support this fact. In the illustration below, a State shared service center federates across multiple governmental services. In doing so, it must establish the role of the identity requesting actions from the services center.



The illustration above show how the Citizen Token contains different attributes than an Employer Token even though it could be the same individual. The Identity Service has the ability to establish identity and role on an inbound request. This makes for an authorized and secure message being sent to the federated service providers. The service provider would also validate identity and role within their domain and may even prompt for more attributes if needed.

4.10 Federation Framework: Standards

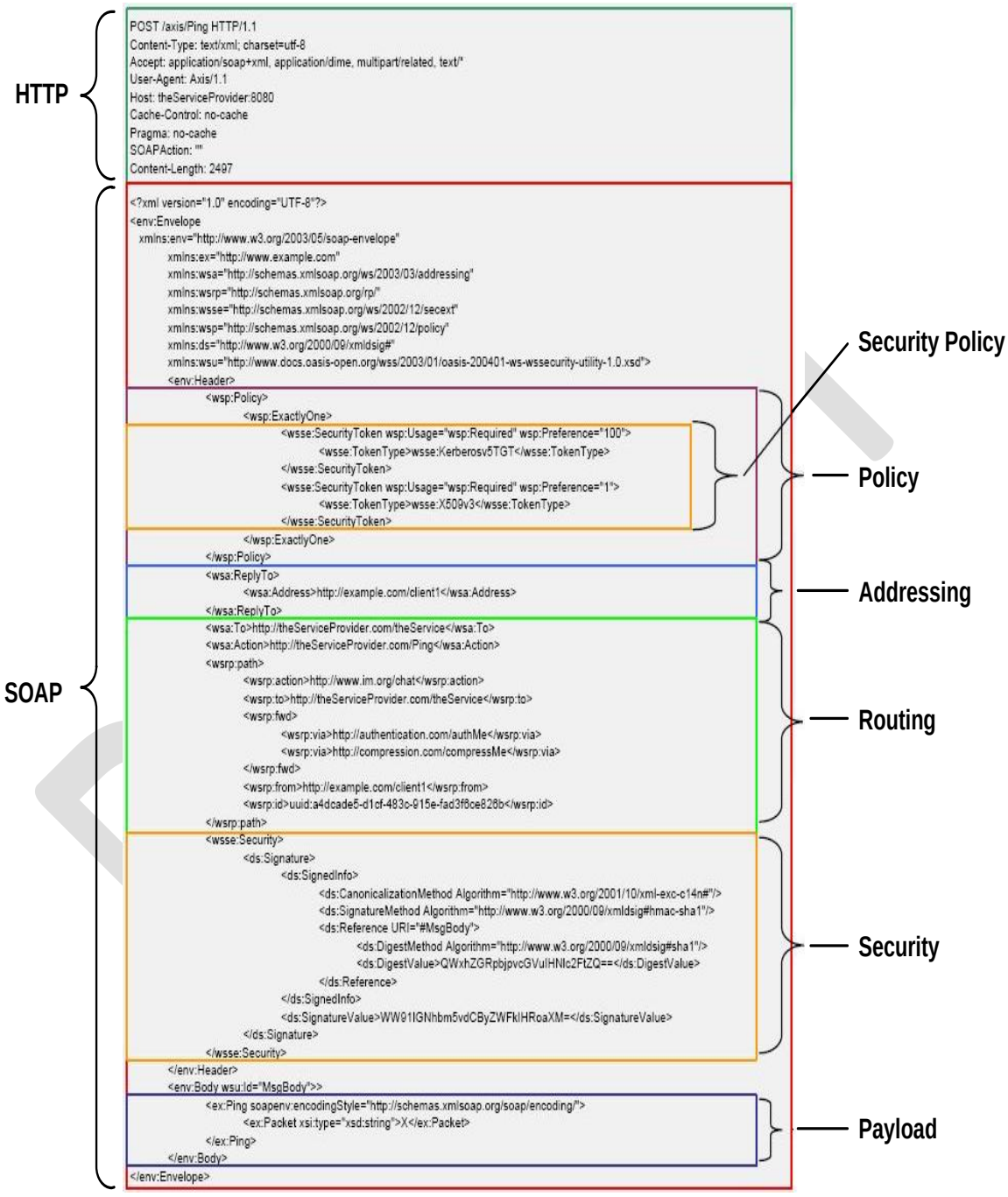
There will be debates over which identity standard is best for years to come; however, this will not inhibit the implementation of federated identity and shared services. The WS-Federation along with OASIS and W3C will continue to merge and refine security and messaging standards. The State has positioned itself to standardize on WS-Federation and SAML standards, but is prepared to embrace other standards as needed. This is not a technical discussion as much as it is a governance issue. Reducing the number of standards within a federated framework provides effective management control over Identities and Messaging. The cost of technical design and support is greatly reduced as well.



This illustration recognizes the multiple spheres of a federated framework in State government. This is only an example and it is understood that there are many more communities of interest that will participate in the Statewide Federated Framework.

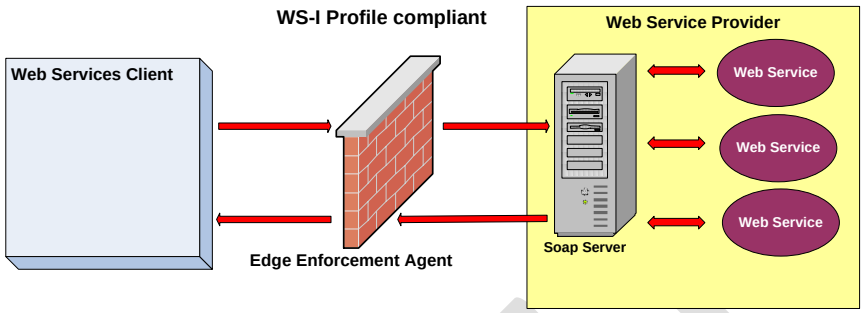
4.11 The Use of A Standard

SOAP Graph



4.12 Firewall Functionality

Firewall Graph.



The Edge agent must look inside the SOAP/WSS messages and enforce security access to the SOAP server.

5. IMPLEMENTATION STRATEGY

In this section, the federated identity management reference architecture outlines the target framework that the SICAM must fit within. This section will also outline how interoperability will occur to share identity attributes across agency boundaries in an effort to reduce the total cost of ownership for agency identity systems and to improve the identity assurance levels for agencies that leverage these services.

5.1 Transition Strategy

This transition strategy describes the proposed rollout of the IDM Reference Architecture to the community. While it has been identified that a roll-out of this architecture would benefit other enterprises, those transition strategies would be developed separately, though could leverage this framework.

5.1.1 Risk Assessment

Improper authentication of users can result in direct and dire consequences to an application, system, and organization. This guide has been developed to assist users in selecting an appropriate level of authentication to resist threats to their data, users, and organizations that could result from unauthorized use of system transactions. This approach emphasizes the development of authentication requirements based on risk. It is designed to approach the task from a business perspective, identify organization risk, then match those risks to the appropriate technical solution. This is accomplished through a risk assessment for each transaction. The assessment identifies:

- risks, and
- their likelihood of occurrence

This section outlines the steps agencies should take to conduct a risk assessment of the e-government system.

1. Data Security Classification Analysis
2. Impact Assessment
3. Likelihood Assessment
4. Calculate Risk Rating
5. Determine Security Level

From the Risk Assessment, agencies can then determine the appropriate Assurance Level for the data or transaction in question, as well as appropriate levels of Identity Proofing and related Authentication Technologies.

To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

1. Potential harm or impact
2. The likelihood of such harm or impact

5.1.2 Step 1 - Data Security Classification Analysis

At the outset, Agencies must baseline the data that they are responsible for by performing a data security classification analysis of internal data and systems. A formal data governance process should be implemented to ensure that a common framework is employed for data lifecycle management. The framework is intended to enable consistent processes and methods for determining and implementing data standards, care, security, ownership, sharing and lifecycle management. The State of Colorado enterprise data governance framework is currently being formulated by the Governor's Office of Information Technology (OIT) and the Office of Cyber Security (OCS).

Out of the data governance analysis, agency stakeholders should fully understand the confidentiality of the data that they are stewards of, as well as the need to protect the integrity of the data while ensuring appropriate access to the data.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are:

- Low impact
- Moderate impact
- High impact.

5.1.3 Step 2 - Impact Assessment

To determine the appropriate level of criticality and sensitivity, the information owner must first assess the potential impact an authentication error would have.

Table 1. Impact Level Definitions

Category	Potential Impact Level		
	Low/1	Moderate/2	High/3
Inconvenience or distress	At worst, limited, short-term inconvenience or distress to any party.	At worst, serious short-term or limited long-term inconvenience or distress to any party.	Sever or serious long-term inconvenience or distress to any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).
Financial loss	At worst, an insignificant or	At worst, a serious unrecoverable	Sever or catastrophic unrecoverable

	inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	financial loss to any party, or a serious agency liability.	financial loss to any party; or severe or catastrophic agency liability.
Harm to agency programs or public interests	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness, or (ii) significant damage to organizational assets or public interests.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) severe mission capability degradation to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Unauthorized release of information Confidentiality	The unauthorized access or disclosure of information would have minimal or no impact to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized access or disclosure of information could have only limited impact to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized access or disclosure of information could severely impact to the organization, its critical functions, employees, third party business partners and/or its customers.
Integrity	The unauthorized modification or destruction of information would have minimal or no impact to the organization, its critical functions, employees, third party business	The unauthorized modification or destruction of information would have only limited impact to the organization, its critical functions, employees, third party business	The unauthorized modification or destruction of information could severely impact the organization, its critical functions, employees, third party business partners and/or its

	partners and/or its customers.	partners and/or its customers.	customers.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Personal safety	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
Civil or criminal violations	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

A risk analysis is to some extent a subjective process, in which the information owner must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. The information owner should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process.

Table 2. Example Assessment, Step 2

Security Level Assessment for Authentication				
Categories of Harm	Impact (Step 1)	Likelihood (Step 2)	Risk Rating (Step 3)	Security Level (Step 4)
Inconvenience, Distress, or Damage to Standing/Reputation	3			
Financial Loss or Agency Liability	3			
Harm to Agency Programs or Public Interests	2			
Unauthorized Release of Information	2			
Personal Safety	N/A			
Civil or Criminal Violations	2			

N/A = No Impact; 1 = Low Impact; 2 = Moderate Impact; 3 = High Impact

5.1.4 Step 3 - Likelihood Assessment

The second step determines the likelihood that an asset would be misused if not properly secured. The information owner must also determine the likelihood that a risk will materialize and that the impact occurs.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls
- Past history

Likelihood should be defined in concrete terms such as impacts are likely to occur daily, weekly, yearly, every decade, or "once in a career". The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as low, medium, or high. Table 3 below describes these three likelihood levels.

5.1.5 Step 4 - Calculate Risk Rating

The next step is to combine impact and likelihood to establish an overall risk rating. This can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example,

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low.
- The value assigned for each impact level is 3 for High, 2 for Medium, and 1 for Low.

Likelihood	Impact		
	Low (1)	Medium (2)	High (3)
Low (0.1)	1 x .1 = .1	2 x .1 = .2	3 x .1 = .3
Medium (0.5)	1 x .5 = .5	2 x .5 = 1	3 x .5 = 1.5
High (1.0)	1 x 1 = 1	2 x 1 = 2	3 x 1 = 3

Therefore, to understand in numerical terms the risk rating for each factor, the following calculation is used: impact x likelihood = risk rating, where the value for the probability factor (0.1, 0.5, 1.0) is substituted for the likelihood numerical 1-3 ranking done in Step 3. Taking the "Inconvenience, Distress, or Damage" category, this formula becomes 3 (for High) x .5 (for 2/Med) = 1.5.

Table 5. Example Assessment, Step 4

Security Level Assessment for Authentication

Categories of Harm	Impact (Step 1)	Likelihood (Step 2)	Risk Rating (Step 3)	Security Level (Step 4)
Inconvenience, Distress, or Damage to Standing/Reputation	3	2	1.5	
Financial Loss or Agency Liability	3	3	3	
Harm to Agency Programs or Public Interests	2	2	1	
Unauthorized Release of Information	2	1	.2	
Personal Safety	N/A	N/A	N/A	
Civil or Criminal Violations	2	2	1	

5.1.6 Step 5 - Determine Security Level

The Security Level defines the results of the Security Level Impact Assessment table's Risk Rating to identify the appropriate Security Level for each Category of Harm.

Security Level	
Risk Scale	Level of Security
Up to .3	Low
>.3 to 1.5	Medium
>1.5 to 3	High

Table 6 below shows our sample completed Security Level Assessment for Authentication.

Table 6. Example Assessment, Step 5

Security Level Assessment for Authentication				
Categories of Harm	Impact (Step 1)	Likelihood (Step 2)	Risk Rating (Step 3)	Security Level (Step 4)
Inconvenience, Distress, or Damage to Standing/Reputation	3	2	1.5	High
Financial Loss or Agency Liability	3	3	3	High
Harm to Agency Programs or Public Interests	2	2	1	Medium
Unauthorized Release of Information	2	1	.2	Low
Personal Safety	N/A	N/A	N/A	N/A
Civil or Criminal Violations	2	2	1	Medium

Now that the risks have been identified and their potential impact quantified, this information can be tied to assurance levels and authentication technologies. Agencies should assess their potential impact category outcomes relative to the authentication level, and choose the lowest level of authentication that will cover all of potential impacts identified.

5.2 Determine Assurance Level

Transactions, processes, and/or information will be classified by the information owner based on its value, sensitivity, consequences of loss or compromise, and/or legal and retention requirements. An appropriate assurance – or trust - level for user credential and authentication must be assigned and implemented to protect the integrity and confidentiality of the information and validity of transactions.

The four trust levels are:

Level	Description
1	Little or no confidence in the asserted identity's validity.
2	Confidence exists that the asserted identity is accurate.
3	High confidence in the asserted identity's validity.
4	Very high confidence in the asserted identity's validity.

Compare the impact profile (Security Level) from the Security Level Assessment to the impact profiles associated with each assurance level, as shown in Table 7 below. Map the potential impacts defined in the Security Level Assessment (Table 6 – step 5) to the four trust levels (1, 2, 3, 4) contained in Table 7. This will identify the level (1-4) of trust required. For example, the "Financial Loss or Agency Liability" category has a security level rating of "High". This translates in Table 7 to a Level 4 Assurance.

Appendix A - Table 7. Maximum Potential Impacts for Each Assurance Level

Appendix B -	Appendix C - Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Additional security controls (audit logging, access right, data validation and verification controls, etc.) should also be implemented for higher trust levels. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

5.2.1 Assurance Level Guidelines

In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some

relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms-to-agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

Associated authentication requirements will be based on the information classification along with any other requirements of the information or transaction being processed. Authentication technologies are determined – and credentials are assigned to users – based on the level of assurance/trust required by the sensitivity of the information and the nature of the transaction.

The four trust levels are:

Level	Description
1	Little or no confidence in the asserted identity's validity.
2	Confidence exists that the asserted identity is accurate.
3	High confidence in the asserted identity's validity.
4	Very high confidence in the asserted identity's validity.

Appendix E: Assurance Level Definitions and Examples contain descriptions and examples of each assurance/trust level.

5.3 Determine Identity Proofing Requirements

The registration and identity proofing process is designed, to a greater or lesser degree depending on the assurance level, to ensure that the agency and/or credential provider knows the true identity of the applicant. Specifically, the requirements include measures to ensure that:

1. A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identity a single person;

2. The applicant whose token is registered is in fact the person who is entitled to the identity;

3. The applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the subscriber's token, the subscriber cannot successfully deny he or she registered that token.

The following text establishes registration requirements specific to each level. There are no level-specific requirements at Level 1. Both in-person and remote registration are permitted for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person registration is permitted at Level 4. Detailed level-by-level identity proofing requirements are stated in Appendix F: Identity Proofing Requirements by Assurance Level.

A credential is evidence attesting to one's right to a privilege or authorization. Credentials can take multiple forms, depending on the transaction, business process, and method of access

(remote or in-person). Applicants are to be vetted to the Table 8 minimum requirements before the appropriate assurance level is assigned and the corresponding credential issued.

Agencies may impose additional vetting requirements such as conducting national background checks, checking criminal history records, terrorist watch list, legal immigration status, and credit history. While these additional checks may be needed to meet specific agency requirements, they have no additional bearing on the assigned proofing level or designated assurance level. Additionally, in some contexts, agencies may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process.
Once an individual is vetted, his/her assurance level is stored as a user attribute in the agency system. Any additional checks required by the agency will also be maintained in the agency system. The personal information used to vet the identity is to conform to all appropriate legislation governing the storage of personal data.

The sensitive data collected during the registration and identity proofing stage must be protected at all times (e.g., transmission and storage) to ensure its security and privacy. Additionally, the results of the identity proofing step (which may include background investigations of the Applicant) have to be protected to ensure source authentication, confidentiality and integrity.

5.3.1 Use of Anonymous Credentials

Unlike identity authentication, anonymous credentials may be appropriate to use to evaluate an attribute when authentication need not be associated with a known personal identity. To protect privacy, it is important to balance the need to know who is communicating with the Government against the user's right to privacy. This includes using information only in the manner in which individuals have been assured it will be used. It may be desirable to preserve anonymity in some cases, and it may be sufficient to authenticate that:

- The user is a member of a group; and/or
- The user is the same person who supplied or created information in the first place; and/or
- A user is entitled to use a particular pseudonym.

These anonymous credentials have limited application and are to be implemented on a case-by-case basis. Some people may have anonymous and identity credentials. Anonymous credentials are appropriate for Levels 1 and 2 only.

5.4 Authentication Technology Selection

All State systems will authenticate the identity of any user prior to allowing any access. All users will be identified to the system by a credential, comprising:

- Unique user-ID; and
- Method of *authentication*.

The level of authentication will be commensurate with the sensitivity of the information being accessed. It is not OIT's position at this point in time to specify which types of authentication

technologies to use, but instead, to provide recommendations and guidelines to assist agencies in determining how to choose the right technology(ies) for their application(s).

This section starts with an overview of the Federal E-Authentication model and the process of authentication, then provides an overview of various types of tokens and the appropriate token type to use based upon the assurance level determined in the Risk Assessment. Authentication rules must be automatically enforced by the system being accessed.

5.4.1 E-Authentication Model

In accordance with [OMB 04-04], e-authentication is the process of establishing confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet; however, in some cases access to the network may be limited and access control decisions may take this into account.

E-authentication begins with registration. An Applicant applies to a Registration Authority (RA) to become a Subscriber of a Credential Service Provider (CSP) and, as a Subscriber, is issued or registers a secret, called a token, and a credential that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.

The Subscriber's name may either be a verified name or a pseudonym. A verified name is associated with the identity of a real person and before an Applicant can receive credentials or register a token associated with a verified name, he or she must demonstrate that the identity is a real identity, and that he or she is the person who is entitled to use that identity. This process is called identity proofing (See Section 6, Determine Identity Proofing Requirements), and is performed by an RA that registers Subscribers with the CSP. At Level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym. This information assists Relying Parties, that is, parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at Levels 3 and 4.

In this document, the party to be authenticated is called a Claimant and the party verifying that identity is called a Verifier. When a Claimant successfully demonstrates possession and control of a token in an on-line authentication to a Verifier through an authentication protocol, the Verifier can verify that the Claimant is the Subscriber. The Verifier passes on an assertion about the identity of the Subscriber to the Relying Party. That assertion includes identity information about a Subscriber, such as the Subscriber name, an identifier assigned at registration, or other Subscriber attributes that were verified in the registration process (subject to the policies of the CSP and the needs of the application). Where the Verifier is also the Relying Party, the assertion may be implicit. In addition, the Subscriber's identifying information may be incorporated in credentials (public key certificates) made available by the Claimant. The Relying Party can use the authenticated information provided by the Verifier/CSP to make access control or authorization decisions.

Authentication simply establishes identity, or in some cases verified personal attributes (for example the Subscriber is a U.S. citizen, is a first responder, or is assigned a particular number or

code by an agency or organization), not what that identity is authorized to do or what access privileges he or she has; this is a separate decision.

Relying parties, typically government agencies, will use a Subscriber's authenticated identity and other factors to make access control or authorization decisions. In many cases, the authentication process and services will be shared by many applications and agencies, but the individual agency or application is the Relying Party that must make the decision to grant access or process a transaction based on the specific application requirements. These guidelines provide technical recommendations for the process of authentication, not authorization.

5.4.2 Federated Identity Management & Authentication

Federated identity management is the use of trust relationships between separate security domains (organizations) to provide appropriate and secure, seamless authentication for users. This enables organizations to be more agile and efficient while improving user productivity and reducing overhead. It is a long-term goal of the State to implement a federated identity management approach and trust model to enable assurance and authentication of external entities in order to:

- mitigate security and privacy risks by developing trust relationships with communities of interest;
- control costs and risks by eliminating the need for each agency to create and maintain a separate credentialing system for each online application;
- facilitate e-Government services in a meaningful way.

5.4.3 Authentication Systems

Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a voice print or other biometric data)

Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. The system may be implemented so that multiple factors are presented to the Verifier, or some factors may be used to protect a secret that will be presented to the Verifier. For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or the hardware device might include a biometric capture device and uses a biometric to activate the key. Such a device is considered to effectively provide two-factor authentication, although the actual authentication protocol between the Verifier and the Claimant simply proves possession of the key.

Tokens are characterized by the number and types of authentication factors that they use. For example, a password is a token that is something you know, a biometric is something you are, and a cryptographic identification device is something you have. Tokens may be single or multi-factor tokens as described below:

- Single-factor token – a token that uses one of the three factors to achieve authentication. For example, a password is something you know, and can be used to authenticate the holder to a remote system.
- Multi-factor token – a token that uses two or more factors to achieve authentication. For example, a private key on a smart card that is activated via PIN is a multi-factor token. The PIN is something you know and the smart card is something you have.

5.5 Attribute Management

Section Description	State Identity, Credential, and Access Management (SICAM) implementation involves integration with multiple partners in a trust network. This section the attribute exchange architecture for identity information. This includes sharing limited user attribute information, providing attribute validation services, and preventing access to sensitive user information.
Intended Audience	▪ State Policy Makers ▪ State Architects ▪ Department Policy Makers ▪ Department Architects ▪ Department Application Owners

An Identity attributes service plays an important role in Statewide Identity Services federation. User attributes can carry authorization information for departments to use within their applications. Attribute exchange and validation across departments are needed for departments to define their security policies and application entitlement services. Even though an authorization service must be managed inside each department's security domain, cross-domain federation among departments through centralized statewide Identity management system provides a certain level of attributes exchange and attributes validation which is the key capabilities of the Attribute Service. Security policies must be provided to protect the attributes which contains sensitive or privacy information. The State of California privacy policy or FIPPS must be followed in any attribute exchange and validation practice. End to end security solutions must be provided to the attribute service to meet the security and privacy requirement of state of California.

5.5.1 User Attribute Service at Department Level

Each department maintains its own identity service which includes user attribute management. The department specific authoritative user attributes can only be retrieved or validated from the department based on the trust model and security measures. The department attribute service must provide a standard based attribute retrieval and validation service to other departments based upon the configured trust agreements established with other departments.
The department user attribute management process must be fully integrated with department Identity management solution which provides an identity life cycle management solution that effectively manages the user attribute creation, change, and deletion. The department IDM

solution must enforce the authenticity of the attributes through its business process in order to provide an authoritative attribute service to other departments.

5.5.2 User Attribute Service at State Level

The centralized Statewide Identity Services is responsible for ID validation and rationalization across departments and also issuing statewide unique identifiers for individuals. The centralized Statewide Identity Services provide PIV-I card registration service to employees and password token registration service for citizens. The State maintains a central correlated user registry (SWUID). Certain user attributes are maintained in this registry, for example, the unique identifier, and department issued unique ID's, basic information about the user, and biometric information about the PIV-I card holders.

When needed, the centralized Statewide Identity Services must be able to provide user attributes or validate user attributes from the central user registry in a trusted and secure manner.

5.5.3 Establish mechanisms and infrastructure for attribute retrieval / exchange

Attributes can be retrieved and exchanged through different mechanisms based on the protocols and standards the departments and state centralized identity system have leveraged.

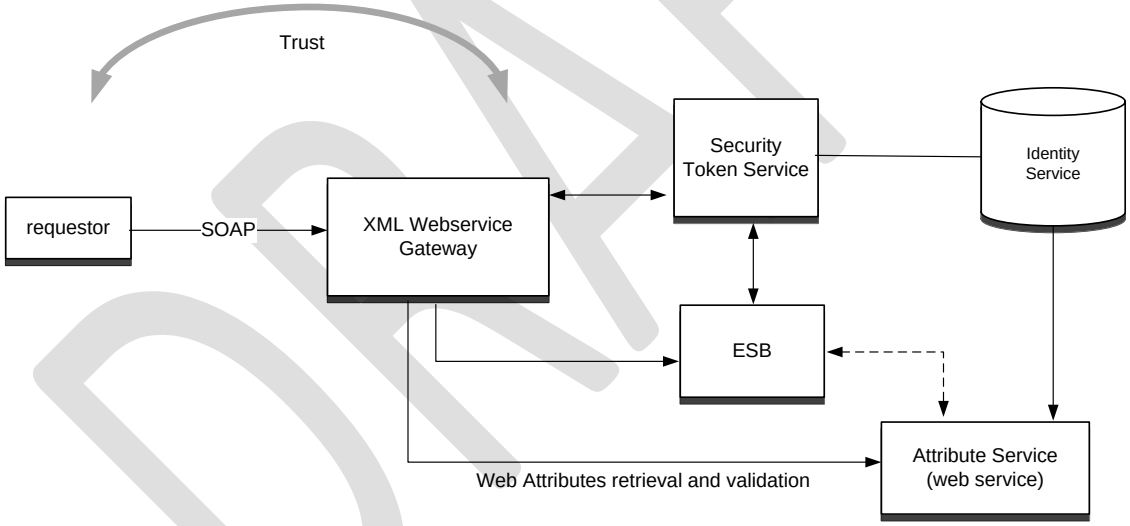


Figure 1 – Attribute Service Architecture

5.5.4 Via SAML token profile (through FSSO)

OASIS SAML2.0 FSSO profile and SAML2.0 token profile [...reference to OASIS…] have defined the protocol and standard for attribute exchange during federated SSO:

If a user is required to authenticate to the state centralized identity system through federated SSO protocol when they are trying to access a department's web application, the state centralized identity system authenticates the user and creates a trusted assertion that contains user attributes and sends this assertion to department to consume. The assertion MUST contain the user's department issued unique ID, along with other attributes based on the business agreement. Departments must be able to consume the assertion and extract

the attributes based on the trust model and security measures. These attributes may be used for authorization service controlled in department.

For example, a user is trying to access an EDD web application which requires authentication through a state centralized identity system, the user's web browser is redirected to state centralized identity system for authentication. After the user is authenticated successfully by providing their unique identifier, password, the state centralized identity system Identity Provider creates a SAML assertion which contains his EDD unique ID and other attributes, such as address, DOB, etc, and sends the SAML assertion to EDD site through FSSO protocol.

5.5.5 Via Backend Attribute Exchange (BAE) SAML profile (through web service)

The federal government requires a standard mechanism for relying parties, (federal agencies) to obtain PIV-I Cardholder information (Backend Attributes) directly from the authoritative source (Attribute Authority). The authoritative source is the state centralized identity service (PIV-I Card Issuer). Access to Backend Attributes is either in real-time when immediately needed (e.g., guard suspects PIV-I Card tampering), or in advance if need. In addition to PIV-I card holder, individuals who only have a password token to access a department resources that may require further information or information validation from an authoritative source. This is typically the department that manages the individual's profile. The standard approach to retrieve or validate the attributes needs to be established within department site as well.

BAE is a general concept pertaining to exchange of PIV-I Cardholder information in a secure and trusted environment between an Attribute Authority (AA) and a SAML 2.0 service provider. The Security Assertion Markup Language (SAML) based exchange of Backend Attributes for one PIV-I Cardholder per request/response pair. The same attribute exchange mechanism should apply to generic individuals who have other form of credentials other than PIV-I card. The attributes supported in the State of California central identity system and departments must be defined to support the existing PIV-I card attributes. The unified Attribute Service with standard interface provides the following functions to all trusted parties in state of California:

1. Attribute Service is a web service component with a published WSDL. It can be optionally integrated with department ESB and has to comply with the department web service security policy.
2. The requestor MUST have trust relationship with the attribute service based on the trust model defined in SICAM. All attribute service invocations must be validated, audited before the service is provided.
3. Attribute service must comply with SAMLV2.0 Request/Response Protocol [SAML2Core] for attribute retrieval.
4. Attribute service must comply with The SAML2.0 profile of XACMLv2.0 [XAC-SAML] for attribute validation. It is highly desired that department has the capability to provide attribute validation, instead of attribute retrieval due to privacy issue.

5.5.6 Maintain security and privacy during attribute retrieval/exchange

When sensitive Personally Identifiable Information (PII) data is exposed for an attribute retrieval service, privacy protection must be enforced in

a. Secure connection between requestor and attribute service. SSLv 3.0 [SSL] or TLS v1.0 [RFC2246] and a strong cipher (of at least 128 bits) MUST be selected to secure the connection.

b. If SOAP message is not signed, <samlp:AttributeQuery>, <saml:Assertion> and <samlp:Response> MUST be signed to provide data integrity and non-repudiation service.

c. Optionally, SOAP message, <saml:Subject> in the request and <saml:Assertion> in the response can be encrypted.

The security is based on the proposed trust model described in previous section.
Privacy protection must be enforced in:

a. Secure connection between requestor and attribute service. SSLv 3.0 [SSL] or TLS v1.0 [RFC2246] and a strong cipher (of at least 128 bits) MUST be selected to secure the connection.

b. If SOAP message is not signed, <samlp:AttributeQuery>, <saml:Assertion> and <samlp:Response> MUST be signed to provide data integrity and non-repudiation service.

c. Optionally, SOAP message, <saml:Subject> in the request and <saml:Assertion> in the response can be encrypted.

5.5.7 Establish State Level Attribute Classification

The attributes which are collected, maintained, and exposed as part of a user lifecycle management process are specific to the business requirements of the state. This section describes several examples of user types and attributes classification on those users which dictate the storage and sharing of user attribute information within the Statewide Identity Services trust framework. User attribute information is comprised of both publically available as well as sensitive PII information. There are three types of attributes which should be considered when defining the attribute classification for user information. These types are listed below.

1. Basic – The attributes reflects the basic information about the user. These attributes can be shared among departments and can be used for identity data correlation. These attributes can be retrieved through trusted attribute service
2. Intermediate – The attributes are unique to the business of departments and can be shared among certain departments based on business agreement and trust model. In most cases, these attributes can only be validated through attribute service. However, in some business transactions, they can be retrieved from the department through trust attribute service.
3. Advanced – These are highly private attributes which are stored in department identity registry. These attributes are only used in department and should never be shared with other departments without user's consent.

There are several different types of users which are maintained by the state. This includes employees, first responders, and citizens as well as other types of users. The following table describes several examples of user attributes which are relevant for citizens as well as first responder user types as well as the corresponding attribute classifications for the user types.

See Appendix XX-Example identity Attributes for further details.

5.6 Governance

The SICAM Governance section is intended to provide an authority guiding trust decisions, definitions, and processes. The governance section defines the SICAM trust model, details frameworks leveraged in development, and explores the relationships around metadata, attributes, and identities. Additionally, this section highlights legislative and policy directives that give rise to the need for development and support of SICAM infrastructure and processes to support the State's missions.

The Federated Identity Management model is based on a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.

Furthermore, it is an architectural style for a community of providers and consumers of services to achieve mutual value9 , that:

1. Allows participants in the communities to work together with minimal co dependence or technology dependence
2. Specifies the contracts to which organizations, people and technologies must adhere in order to participate in the community
3. Provides for business value and business processes to be realized by the community
4. Allows for a variety of technologies to be used to facilitate interactions within the community

Effective operations of such model for the State would require a high level of coordination between various departments under a governance model compatible with objectives and design of SICAM.

There are a number of universal frameworks, standards, and best practices for governing IT projects such as:

- Control Objectives for Information and related Technology (COBIT)
- IT Infrastructure Library (ITIL)
- Various ISO/IEC standards – 38500:2008, ISO 27001

This section describes a high-level governance model-using example of The Global Federated Identity and Privilege Management Initiative (GFIPM). GIFPM is a collaborative effort of the Global Justice Information Sharing 4 Initiative (Global) membership, the United States Department of Justice (DOJ), Office of 5 Justice Programs (OJP), Bureau of Justice Assistance (BJA), and the U.S. Department of 6 Homeland Security10.

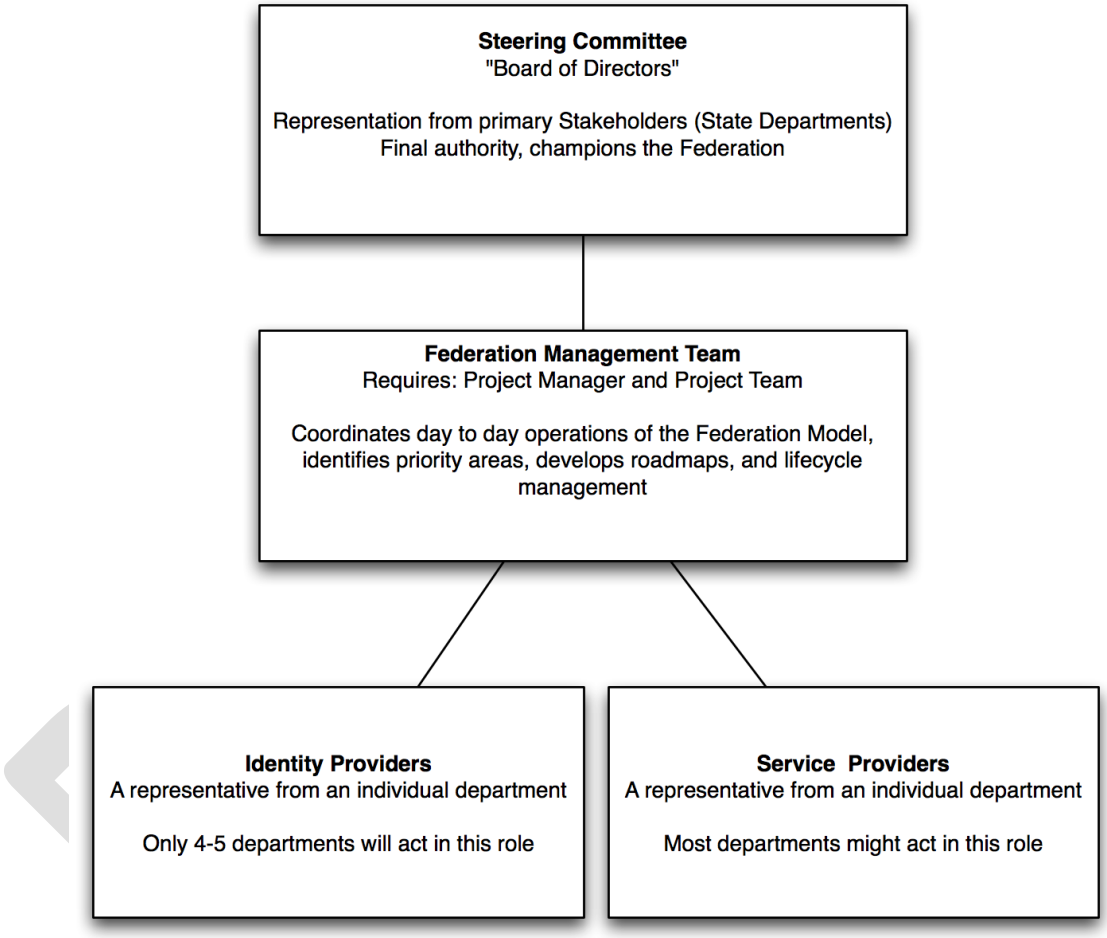
[9] This observation is based on OMG definition of Service Oriented Architectures

[10] For more information visit http://www.it.ojp.gov/GFIPM

5.6.1 Establish Governance Authority

Below is a high-level organizational structure example for establishing Federated Identity Management governance authority. This example is based on the GIFPM governance model. We provided some adjustments to reflect State of California specific organizational design – specifically the fact that there might only a handful of Identity Providers and majority of departments will act as Service Providers.

Figure 2: High Level Governance View Diagram



Description of specific roles, key activities, and responsibilities of various parties is provided in Appendix F) Example of Roles and Responsibilities

5.6.2 Manage Lifecycle of Common Specifications and Standards

Source: CalDRM draft documentation

The management of common specifications and standards consists of five high level processes represented in Figure 3 below.

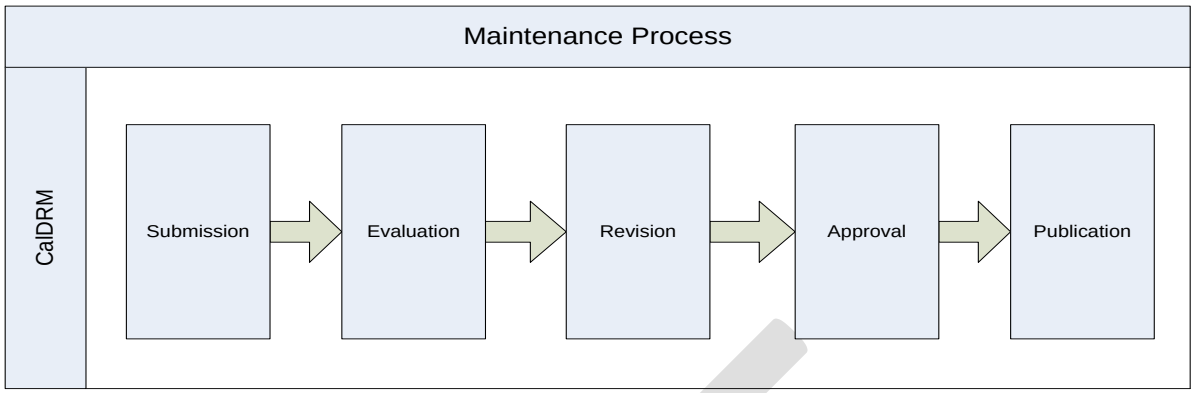


Figure 3: CalDRM high-level process for metadata management

- Submission – Departments submit revisions/modifications to the reference model(s) to the Federation Management Office for consideration.
- Evaluation – The FMO collects, reviews, and screens the submissions based on standardized evaluation criteria.
- Revision – The FMO forms a team to perform analysis and develop the revised Metadata Model.
- Approval – The Steering Committee reviews the final version for publication.
- Publication – The FMO publishes the revision.

Governance Entity	Role
Steering Committee	▪ Charter the Enterprise Architecture and Standards Committee ▪ Ensure alignment with the California State Information Technology Strategic Plan
Federation Management Office (FMO)	▪ Review and approve DRM revisions ▪ Collaborate with other committees to ensure alignment and consistency with the California Enterprise Architecture Collect, review, and evaluate the submissions based on standardized evaluation criteria ▪ Form team(s) to perform analysis and develop the revised SICAM Metadata Model ▪ Review and revise the SICAM Metadata ▪ Publish the revision(s)
Department – Identity Provider / Service Provider	▪ Serve as submitters of potential modifications to the reference models ▪ Supply Subject Matter Experts ▪ Provide feedback on reference model revision(s)

Management of attributes on the local domain level (within each State department) and cross-domain level (under the SICAM governance model) requires a governance process. Management of these attributes and artifacts associated with them is one of the key elements of the Federated Identity governance model.
Some of artifacts required to be managed by the Federation Management Office are listed in the table below.

Metadata Layer	Description
Federation Profile	▪ A profile of the conceptual model that addresses the needs of a specific federation instance ▪ Places subset and constraint rules on the abstract federated user and federated entity models as needed ▪ Represented by a set of schemas that specify a subset of the schemas used to define the conceptual model
Federation Profile Instance	▪ XML instance that conforms to a specific federation profile ▪ Encapsulates the metadata (data payload) for a specific authenticated federation user or federated entity conforming to the federation profile schema
SAML Assertion	▪ Acts as the transport mechanism for the XML instance between an identity provider and a service provider
XML Schemas	▪ Contains the official schema-level specifications of the metadata model
SAML 2.0 Encoding Rules	▪ Contains rules for encoding metadata into SAML 2.0 profile

5.6.3 Establish IDP and SP Certification, On-boarding and Membership Process

Part of the SICAM framework is to identify a process for a State department to apply for Identity Provider Certification. A department that manages a specific population of identities should be able to apply and be considered an authority for these identities. Part of the process of establishing the new identity provider is to identify business reason and validate value of contribution of these identities from the service provider perspective. In other words a department who can provide or validate certain attributes associated with identities should be allow to become Identity Provider only if specific business case exist and there is a demand from the Service Provider community to consume these identities.

This process can be formalized by Federation Management Office and evaluation criteria need to be established by the steering committee to evaluate prospective identity providers.
A typical process for joining the Federated Identity Management consists of the following steps:

1. Request-to-Join Process

2. Application Process
3. On-boarding Process
4. Ongoing Membership

For example the GIFPM framework describes the following content of application to join packaged required to be completed by each Identity Provider candidate.

The IDP application package consists of the following contents:

a) **Completed Application Form** – a standard form on which an organization provides basic organization information about itself, e.g. name, address, names, and titles of its organizational officers, etc.
b) **Signed IDP Agreement** – an agreement signed by an IDP to indicate its intent and willingness to abide by the governance and rules of the Federation
c) **Authority-to-Operate Document** – a document attesting to the organization's authority to operate as an identity provider for users under a specific legal jurisdiction
d) **Local Security Policy Document** – a document describing the security policy that is currently in place within the organization
e) **Local User Agreement Document** – a document describing the terms and conditions to which users must agree as a prerequisite for using a digital identity issued by the organization
f) **Local User Vetting Policies & Procedures Document** – a document describing the user vetting policies and procedures that are currently in place within the organization
g) **Completed Local Attribute Mapping Form** – a document describing how the organization plans to map its local policies and locally stored user attributes into attributes conforming to the GFIPM Metadata standard.
h) **Completed Security Practices Checklist Form** (based on FIPS 200) – a checklist that summarizes the organization's local security policy. The checklist is - For Information Only. Applicants are not required to be compliant with all items on the checklist.

Similar to the certification to operate as Identity Provider within the SICAM framework, various departments should be able to apply for Service Provider Certification. The process of justifying a department willing to act as SP can be simplified (ability to handle more SPs) when compared to vetting of IDPs.

A standard process of joining as a Service Provider in the GIFPM governance framework consists of the following steps:

a. **Completed Application Form** – a standard form on which an organization provides basic organization information about itself, e.g. name, address, names, and titles of its organizational officers, etc.
b. **Signed SP Agreement** – an agreement signed by an SP to indicate its intent and willingness to abide by the governance and rules of the Federation
c. **Authority-to-Operate Document(s)** – a set of documents attesting to the organization's authority to operate as a service provider and make available electronic resources belonging to, or under the legal control of, a specific legal jurisdiction
d. **Local Security Policy Document** – a document describing the security policy that is currently in place within the organization3

e. **Completed Local Access Policy Mapping Form** – a document describing how the organization plans to map its local access control policies into rules that can be expressed using attributes from the GFIPM Metadata standard
f. **Completed Security Practices Checklist Form** (based on FIPS 200) – a checklist that summarizes the organization's local security policy. The checklist is – For Information Only. Applicants are not required to be compliant with all items on the checklist.

5.6.4 Token Acceptance Policy

After the internal risk analysis of section 3 is done, agencies or enterprises can then choose technologies to support the appropriate security and risk level.. this section should include some information on the work that needs to be done to determine the technology selections based on the risk vs. cost tradeoff.

5.6.5 Trust Policies

This working group should develop guidelines for the types of policies that need to be implemented to enable trust in a digital identity world. Examples of policy types include:

- Establishing a digital identity
    - Identity proofing
    - PIV-I is Level 4, medium hardware assurance as a starting point; ramp up or down as necessary
- Establishing roles in an enterprise that equate to types of information that can be accessed, which helps inform the types of technology tokens and security controls that need to be implemented
- Establish attribute – what are the attributes needed for transition types by relying parties in order to trust the identity. With this concept, we recognize that a person only has one identity, but can have multiple attributes and privileges (e.g., driver, voter, receiver of benefits, employee, first responder, patient) assigned to her or him. The assigning of attributes assigned will remain with the agencies and programs that are serving individuals.
    - Source attribute system identification
- Use of a policy engine to electronically enforce all necessary federal and state statutes

5.7 Maintenance

The IdAM should evolve as the many different agencies incorporate it within their specific EA. Any changes to the plans, projects, and/or reference agency's architecture should be captured in an appropriate documentation trail, and should be justified on the basis of costs, benefits, and risks. Changes should be processed through established change control processes and board

authority. The change documentation should characterize the problem, solution, and alternatives chosen and rejected in light of established priorities.

The preferred method by which the Registration Authority will evolve and mature for use throughout reference agencies is through Communities of Practice (CoP). These CoP's provide an environment where the community or users of the architecture are empowered or own the maturity of the model. These CoP's may decide to meet face to face, via internet, or other collaborative means. The use of a wiki provides the single source owner and approval processes by evaluating community input and real life experiences. This tool can be used in the evolution and adaptation as constant change is addressed. With each community (reference agencies) providing input and feedback to their best practices, the overall model of identity management can be assessed on a regular basis (at least annually) and grow into the appropriate and expected target architecture. Much like the reference models, the reference architecture will mature with changes as feedback and lessons learned are provided.

Individual organizations, on the other hand, will maintain their architecture within the enforcement structure and configuration control mechanisms as any EA. Using a system of oversight processes and independent verification, the reference agency architecture team will periodically assesses and align their specific identity management architecture to the ever-changing business practices, funding profiles, and technology insertions.

The successful maturity of each agency's identity management enterprise architecture should continuously reflect the current state (baseline architecture), the desired state (target architecture), and the long-and short-term strategies for managing the change (the sequencing plan). Below is an illustration of how continuous changes should be addressed. At no time will specific target architectures ever be achieved with each iterative update of the EA, all three components shown in the figure and the timeline are recast. The target architecture is a vision of the future that evolves in advance of it being achieved.

5.8 Communication Strategy

Like any complex project, program, activity or task, there must be solid communications. This is accomplished through a communications plan. This plan will (1) to keep senior executives and business leaders continually informed, and (2) disseminate EA information to management teams as appropriate. The CIOs staff, in cooperation with the Chief Architect and support staff, defines a communications plan consisting of (a) constituencies, (b) level of detail, (c) means of communication, (d) participant feedback, (e) schedule for marketing efforts, (f) working groups like HSPD-12, and (g) method of evaluating progress and buy-in. It is the CIOs role to interpret the agencies vision and to recognize innovative ideas (e.g., the creation of a digital government) that can become key drivers within the EA strategy and plan. If resources permit, the Chief Architect should use one or all of the following tools to communicate with the community of interest: seminars and forums, web pages, electronic surveys, and e-mail list servers.

To meet these general information needs, the Identity Management Reference Architecture Program will implement the following communications tools.

1. The Program will develop a set of basic information materials describing the scope of the statewide Enterprise Architecture. This set of materials will describe the value, benefits, and importance of Enterprise Architecture.. The materials will be brief and concise, and may consist of: one-page briefing or brochure, key concept map, Frequently-Asked Questions (FAQ) document, and PowerPoint presentation.

2. In all status reporting, Committee and Program achievements will be explicitly linked to government-wide business objectives.

3. The basic EA scope and value materials, as well as some high-level business-oriented status information, will be available (and prominently displayed) on an EA website, be it SharePoint, Wiki, or other collaboration tool. These materials should be suitable for use/delivery by EA Committee members as well as program staff.

4. Other means used will be used, such as, phone conferences, Online Collaboration meeting tools, wiki engines, and the internet, to name a few.

The communications plan will also identify stakeholders of the reference agency, the information needs of those stakeholders, and the communication strategy to be followed by the reference EA program in meeting those needs. The enterprise architecture and the operations of the program charged with evolving that architecture are important topics of communication that must be addressed by the program if the enterprise architecture initiative is to succeed.

Effective communication is part of the overall plan for management of the Identity Management Reference Architecture Program. Therefore, this plan references and is referenced by the Identity Management EA Program and each reference agency's management.

5.9 Capital Planning Integration

It is the responsibility of each reference agency executive management to institutionalize the control structures for the EA process as well as for the agency CPIC and SLC processes. For each decision-making body, all members should be trained, as appropriate, in the EA, the EA process, and the relationship of the EA to the CPIC and SLC.

Anyone who might bring forward a proposal to the Capital Investment Council (CIC) such as domain managers and project managers should understand the requirement for EA assessments. To adequately evaluate an investment proposal, the CIC needs specific information. Individuals creating the investment proposals should be trained, as appropriate, in the criteria and submission requirements. Appropriate training will prepare the staff to assess the compliance and correct any deficiencies that exist prior to submission.

Investment management is closely linked with the EA processes. The agency should only make investments that move the agency toward the target architecture and these investment decisions should comply with the sequencing plan. The EA, CPIC, and SLC (systems life cycle) processes are integrated to best suit the agency's particular organization, culture, and internal management practices.

Each agency implementing the IDM model designs its own CPIC process for structuring budget formulation and execution to ensure that investments consistently support strategic goals. All IT projects should align with the agency mission and support agency business needs while minimizing risks and maximizing returns throughout the investments life cycle. The target architecture and the sequencing plan provide information for the three phases of the CPIC process. In Figure 12, the EA swim lane indicates the update of the target architecture.

If an identity management related investment is planned, OMB will ensure that it can be mapped to an element in the reference architecture. OMB 300's may specifically ask whether the investment is identity management related (akin to asking if it is homeland security related), and approve such investments with less scrutiny.

To assess the business alignment of the proposed investment, decision makers use, for example, the business case, acquisition plan, and the project plan to determine whether the proposed investment aligns with the sequencing plan and target architecture. Next, decision makers monitor business and technical compliance as demonstrated in the updated business case, system architecture, systems design, and test program. In addition, the investment should be monitored to ensure continuing alignment with the agency's strategic and business goals, which may shift over time. Finally, the decision makers perform a final assessment to determine technical and strategic compliance with the EA. The results, including findings of noncompliance, should influence strategic planning for new business and IT projects, which could then lead to changes in the EA.

Therefore, the CPIC process should respect the integrity of the sequencing plan while considering the strategic and tactical value of all proposals that pass through CPIC checkpoints. Project critical success factors continue to be met. This double check on project proposals ensures that all funded projects meet the conditions necessary for success. These conditions include, but are not limited to:

Consistency with the EA

- Satisfaction of project baseline cost, schedule, capability, and business value commitments
- Compliance with agency-published investment management policies and guidance
- Explicit support by executive management.

5.10 Architecture Compliance Process

The architecture compliance function will be implemented according to the OCIO EA Policy and Standards outlined in the State Administrative Manual (SAM) and the State Information Management Manual (SIMM). The annual evaluations will cover:

1. Business Performance, as per IdAM maturity model measurement areas
2. Technical Alignment with Enterprise and Agency-level Standards
3. Architecture Alignment

The data collected within the business performance area will be used for reporting to OCIO using their Annual EA reporting templates or tools for reporting EA artifacts. These reports are described further the SIM EA Policy. The remaining portions of the evaluation will be used by agencies internally. By mandating this compliance function, the governing body will be empowering the agency EA program's to drive movement within the agency towards the agreed upon goals.

Agencies who do not make progress or remain compliant may have funds frozen or may be asked to outsource their identity management capability. In most cases, however, the assessment should be used to align investments with IdAM needs and 2) to update the EA models.

6. ROLES

Within a federation, business partners play one of two roles: Identity provider or service provider or both. The identity provider (IdP) is the authoritative site responsible for authenticating an end user and asserting an identity for that user in a trusted fashion to trusted business partners. Those business partners who offer services but do not act as identity providers are known as service providers.

The identity provider takes on the bulk of the user's life cycle management issues. The service provider (SP) relies on the IdP to assert information about a user, leaving the SP to manage only those user attributes that are relevant to the SP.

6.1 Identity Provider – IdP

The identity provider is responsible for account creation, provisioning, password management, and general account management, and also acts as a collection point or client to trusted identity providers. Having one federation business partner act as a user's IdP relieves the remaining business partners of the burden of managing equivalent data for the user. These non-IdP business partners act as service providers (SPs). These service providers will leverage their trust relationships with an IdP to accept and trust vouch-for information provided by an IdP on behalf of a user, without the direct involvement of the user. This enables businesses (service providers) to off load identity and access management costs to business partners within the federation.

To achieve the overall user life cycle management required for a full federated identity management solution, the identity provider assumes the management of user account creation, account provisioning, password management, and identity assertion. The identity provider and service provider cooperate to provide a rich user experience by leveraging distinct federated identity management profiles that together provide a seamless federation functionality for a user.

6.2 Service Provider – SP

A service provider may still manage local information for a user, even within the context of a federation. For example, entering into a federated identity management relationship may allow a service provider to handle account management (including password management) to an IdP while the SP focuses on the management of its user-specific data (for example, SP-side service-specific attributes and personalization related information). In general, a service provider will off-load identity management to an identity provider to minimize its identity management requirements while still enabling full service provider functionality.

The SP will consume the trust vouch-for information (assertion) and process accordingly to provide authorization to the service being provided. It is the SP's responsibility to provide and administer the authorization methods for access resources and services.

7. SICAM USE CASE SCENARIOS

In this chapter we introduce several hypothetical use cases and show how they might be able to take advantage of identity federation to improve customer experiences and reduce cost and improve overall security.

The overview of our architecture for the use cases is as follows:

7.1 Create and Maintain Digital Identity Record for Internal User

7.2 Create and Maintain Digital Identity Record for External User

7.3 Perform Background Investigation for State Applicant

7.4 Create, Issue, and Maintain PIV Card

7.5 Create, Issue, and Maintain PKI Credential

7.6 Create, Issue, and Maintain Password Token Overview

7.7 Provision and Deprovision User Account for an Application

7.8 Grant Physical Access to Citizen, Employee or Contractor

7.9 Grant Visitor or Local Access to State-Controlled Facility or Site

7.10 Grant Logical Access

7.11 Secure Document or Communication with PKI

Use Cases shall be documented when building the authentication services in the State of California Federated Trust Domain Model as described within.

8. CONCLUSION

There are many steps along the way and an organization may find that not all of the areas fit neatly within the lines. Maturity within the architecture framework will vary across the business architecture processes, technology architecture, as well as the architecture blueprint. This is an ever-evolving process in the life of all organizations that leads to an efficient, effective responsive development and support organization for Identity and Access Management Solutions.

The SICAM is a development framework, illustrating basic Enterprise Architecture methodologies and approaches for implementing an Enterprise IdAM solution. It contains templates to be used in the process and samples of real cases, which were compiled from the input of several state and local representatives.

It is through the architecture frameworks and framework elements that the SICAM provides state and local governments the means to apply adaptive enterprise architecture, which aids in a structured and consistent delivery of services and information.

The SICAM not a document that you produce once, store on the shelf and reference on occasion. It is a plan and a methodology; it must be both or it has no value. Just as with city plans and building codes, it is constantly being renewed and updated to meet the demands on the organization. There will be good decisions and bad decisions on the way, but having the information surrounding the decisions captured allows for better analysis for future decisions.

We encourage you to use all the tools developed under NASCIO's guidance. Enterprise Architecture is a key success factor to an organizations ability to plan and react to the many mandates and challenges presented to international,

9. APPENDIX - ACRONYMS

Acronym	Description
AAES	Authoritative Attribute Exchange Service
ADS	Authoritative Data Source
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BAE	Backend Attribute Exchange
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CRL	Certificate Revocation List
CSP	Credential Service Provider
CVS	Clearance Verification System
DA	Data Administrator
DBMS	Database Management System
DOB	Date of Birth
EA	Enterprise Architecture
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GUI	Global Unique Identifier
HR	Human Resources
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Identity Access Management
ICAM	Identity, Credential & Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
ID	Identification
IDMS	Identity Management System
IDP	Identity Provider
ISE	Information Sharing Environment
ISIMC	Information Security and Identity Management Committee
ITAA	Information Technology Association of America

JPAS	Joint Personnel Adjudication System
KRA	Key Recovery Agent
LACS	Logical Access Control Systems
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Agent
NCES	Net-Centric Enterprise Services
NIEM	National Information Exchange Model
NIST SP	National Institute of Standards and Technology Special Publication
NPE	Non-Person Entity
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol

10. APPENDIX - GLOSSARY

Term	Definition
Adjudicator	Provides adjudication of background check information to determine eligibility of the applicant to receive a credential, access rights, or be able to work for the State Government as an employee or contractor.
Adjudication	Evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: □ suitable for State Government employment; □ eligible for logical and physical access; □ eligible for access to classified information; □ eligible to hold a sensitive position; or □ fit to perform work for or on behalf of the State Government as a contractor employee.
Applicant	Individuals that request issuance of a credential or access to an application. An applicant becomes a credential holder after issuance and a user after being granted access to an application.
Application Administrator	The party responsible for the maintenance and implementation of access control rights. Application Administrators should not be the approvers due to separation of duties.
Attribute Authorities	An entity recognized as having the authority to verify the association of attributes to an identity.
Authentication Credential	A type of authenticator possessed by a user that provides a strong mechanism used to prove the credential holder's identity. Examples include a PKI certificate or a PIV card.
Authenticator	A memory, possession, or quality held by a person that can serve as proof of identity when presented to a verifier.
Authoritative Attribute Exchange Service (AAES)	Service that performs discovery and mapping of attributes from authoritative source repositories.
Authoritative Data Source	The repository or system that contains the data and attributes about an individual that are considered to be the primary source for this information. If two systems with an individual's data have mismatched information, the authoritative data source is used as the most correct.
Authorizer	Approves or denies access to applications or facilities based on business rules.
Biometrics	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Card Management System	An application that manages the issuance and administration of multi-function enterprise access smart cards. The CMS manages cards, as well as data, applets and digital credentials, including PKI certificates related to the cards throughout their lifecycle.
Cardholder/Credential Holder	An individual possessing an issued token, PKI certificate, PIV Card or other authentication device.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
Certificate Revocation List (CRL)	A composite list of all expired and revoked certificates issued from a CA that can be used to verify the current status of a PKI certificate.
Certificate Status Servers	The counterpart to the Certification Authority that passes revocation and expiration status to relying parties in real time.
Citizen	A citizen for purposes of this document is strictly used to describe a human inhabitant within the State, whether or not they are considered a legal citizen and/or entitled to rights or services provided by the State.
Clearance Verification System (CVS)	A State repository for authorized personnel to determine whether an appropriate background investigation has been performed.
Core Identity Attributes	Attributes that are specific to an individual and, when aggregated, uniquely identify a user within and across agency systems. Core Identity Attributes are also the list of attributes that agencies must make available to one another to enable federation of identity records.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Credentialing Determination	Determination of whether or an individual is eligible to receive a PIV credential as either a State employee or contractor.
Data Administrator (DA)	An individual responsible for maintaining an organization's data and establishing relationship between authoritative data repositories. The individual may also be an application administrator responsible for managing local data.
Domain Controller	The server(s) that manages passwords and authentication requests for a set of applications.
Digital Identity	The representation of Identity in a digital environment.
E-Authentication Assurance Level (EAAL)	Evaluation categories by which authentication mechanisms are measured based on NIST SP 800-63. The lowest level assurance is 1; the highest level assurance is 4.
Enrollment Officer	The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind an Applicant to his/her biometric, and validate identity documentation. The Enrollment Officer delivers a secured enrollment package to the IDMS for adjudication.

External Identity Provider (IDP)	A service or system that establishes an individual's identity and links the identity to a physical or electronic credential or token. IDP's validate the identity of the individual using the credential or token issued and pass along verification of the individual's identity to a relying party, usually through a SAML assertion. Within this Use Case, External IDPs are agency systems, other than the agency performing the validation. External IDP's are those systems or services that are not directly controlled or managed by the agency.
External System or Third Party Application	Resources maintained and operated by a separate state agency, the private sector, or another third party outside of the agency.
External User	Any individual attempting or requesting access to agency facilities or systems that is not an employee, contractor, or primary affiliate of the agency. External users may be PIV holders from another agency, business partners, or private citizens.
Global Federated Identity and Privilege Management (GFIPM) framework	An initiative that provides the justice community and partner organizations with a standards-based approach for implementing federated identity management using the concept of globally understood metadata. GFIPM utilizes direct trust across participating agencies.
Government-to-Business (G2B)	G2B is the online non-commercial interaction between local and central government and the commercial business sector, rather than private individuals.
Government-to-Citizen (G2C)	G2C is the electronic interaction between citizens, or private individuals and government resources
Government-to-Government (G2G)	G2G is the electronic interaction between Federal, State, City, County, and tribal Government agencies.
Integrated Automated Fingerprint Information System (IAFIS)	A national fingerprint and criminal history system maintained by the FBI, Criminal Justice Information Services (CJIS) Division that provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.
Identity	The unique biological person defined by DNA; the physical being.
Identity Management (IdM)	The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguard of personal identity information.
Identity Management System (IDMS)	An automated system of hardware (servers) and software (programs) that provides the workflow management (services) of identity functions, as normatively described in FIPS 201. An IDMS is separately layered and/or compartmentalized within one system and/or a modular component of an agency's centralized system/enterprise. The IDMS will be encapsulated in an environment that is secure, auditable and protect the privacy of personal information. The IDMS establishes the centralized Chain-of Trust that is then integrated into the components of a FIPS 201 compliant enterprise.

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information use by an agency. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources provided by the agency, or outside service providers on behalf of the agency.
Internal/Agency/Local Application or System	A logical system, software or other application in which access is controlled by a particular agency. Internal systems are those hosted, managed, or otherwise controlled by the agency. These systems may only be available within the agency networks and behind agency firewalls.
Internal Actors	Individuals (users, applicants, credential holders, etc.) that primarily consist of employees and contractors of an agency, but also include any fellows, interns, researchers or other individuals tightly affiliated with an agency. These are users who have a primary affiliation to the agency, and for whom the agency typically collects digital identity records and provides credentials for access to agency IT resources or buildings.
Investigative Service Provider (ISP)	An entity responsible for collecting and processing personal investigative data, performing various checks, and providing investigative results to the requesting agency.
Investigator	An authorized individual who performs background investigations on behalf of an Investigative Service Provider.
Issuer	The entity that issues a credential to the Applicant after all identity proofing, background checks, and related approvals have been completed, especially for, but not limited to, PIV and PKI credentials.
Federation	A trust model formed among a collection of Identity Providers and Service Providers spanning multiple department organizational boundaries.
Board of Directors	This is the executive level body with representation from primary stakeholders that guides the federation and is the final authoritative body to make decisions for the federation.
Federation Management	This is the body that manages the day-to-day operations of the Federation, including developing and maintaining standards, membership coordination and providing executive secretariat services to the Board of Directors.
Federation to Federation	The establishment of an inter-federation trust model between like and unlike federations.

Identity Providers	An entity that vets individuals, collects attributes about these individuals, maintains these attributes in an accurate and timely manner. The IDP performs user authentication each time an individual presents themselves to the federation and assigns the current attributes about the individual for a given information technology session. These attributes are presented to Service Providers in the Federation or on a federation-to-federation basis.
Service Providers	A federation member organization that provides one or more electronic information service(s) to the Federation. Service providers' services evaluate the set of Identity Provider attributes presented to the SP in a form that is consistent with the SICAM Interface Control Document (e.g. SAML assertion) to determine what access to provide or deny to each end user. These definitions below are abstracted from two sources: the OASIS Security Services Technical Committee document Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (available at http://www.oasisopen.org/committees/download.php/11886/oasissstc-saml-glossary-2.0-os.pdf) and the Liberty Alliance Project's Liberty Technical Glossary Version: v1.3 (available at http://www.projectliberty.org/specs/draft-libertyglossary-1.3-errata-v1.0.pdf).
Administrative Domain	An environment or context that is defined by some combination of one or more administrative policies, Internet Domain Name registrations, civil legal entities (for example, individuals, corporations or other formally organized entities), plus a collection of hosts, network devices and the interconnecting networks (and possibly other traits), plus (often various) network services and applications running upon them. An administrative domain may contain or define one or more security domains. An administrative domain may encompass a single site or multiple sites. The traits defining an administrative domain may and, in many cases will, evolve over time. Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries.
Affiliation	In Liberty, an affiliation is a set of one or more entities, described by provider ID's, who may perform Liberty interactions as a member of the set. An affiliation is referenced by exactly one affiliation ID and is administered by exactly one entity identified by their provider ID. Members of an affiliation may invoke services either as a member of the affiliation (using affiliationID) or individually (using their provider ID). Affiliation and affiliation group are equivalent terms.
Affiliation ID	In Liberty, an Affiliation ID identifies an affiliation. It is schematically represented by the affiliation ID attribute of the <AffiliationDescriptor> metadata element.

Assertion	A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject or authorization permissions applying to the subject with respect to a specified resource. As used in Liberty, assertions typically concern things such as: an act of authentication performed by a Principal, attribute information about a Principal or authorization permissions applying to a Principal with respect to a specified resource.
Asserting Party	Formally, the administrative domain that hosts one or more SAML authorities. Informally, an instance of a SAML authority.
Attribute	A distinct characteristic of an object (in SAML, of a subject). An object's attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address and so on. Which attributes of an object are salient is decided by the beholder. See also XML attribute.
Attribute Authority	A system entity that produces attribute assertions.
Attribute Assertion	An assertion that conveys information about attributes of a subject.
Authentication	To confirm system entities asserted principal identity with a specified, or understood, level of confidence.
Authentication Assertion	An assertion that conveys information about a successful act of authentication that took place for a subject. In the Liberty specification suite, an authentication assertion contains a <lib:AuthenticationStatement>. Note that the foregoing element is defined in a Liberty namespace. Also known as Liberty authentication assertion and ID-FF authentication assertion. Liberty authentication assertions are formal XML extensions of SAML assertions.
Authentication Authority	A system entity that produces authentication assertions. In the Liberty architecture, it is typically an identity provider (synonymous with authenticating identity provider or authenticating IdP). An identity provider that authenticated a Principal Authentication, Authorization and Accounting Services.
(AAA)	Three system functions that are the underpinning of a security service: authentication recognizes the user; authorization enforces access controls and delivers services; accounting tracks users' usage of system resources.
Authorization	The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access.

Authorization Decision	The result of an act of authorization. The result may be negative: *that is, it may indicate that the subject is not allowed any access to the resource.*
Authorization Decision Assertion	An assertion that conveys information about an authorization decision.
Bearer token	In Liberty, a bearer token is a form of security token that connotes some attribute(s) to its holder. Typically bearer tokens connote identity and they consist essentially of credentials of some form, e.g. SAML assertions.
Binding, Protocol Binding	An instance of mapping SAML request-response message exchanges into a specific protocol. Each binding is given a name in the pattern "SAML xxx binding".
Circle of Trust (CoT)	A federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment. Also known as a Trust Circle.
Discoverable	A discoverable "in principle" service is one having a service type URI assigned (this is typically in done in the specification defining the service). A discoverable "in practice" service is one that is registered in some discovery service instance. IDWSF services are by definition discoverable "in principle" because such services are assigned a service type URI facilitating their registration in Discovery Service instances.
Discovery Service (DS)	An ID-WSF service facilitating the registration, and subsequent discovery of, ID-WSF service instances. See also discoverable.
ID	A shorthand designator referring to the Liberty ID-WSF, ID-FF and ID-SIS specification sets. For example, one might say that the former specification sets are all part of the Liberty ID-* specification suite. ID-* fault message – A SOAP <S:Fault> element containing a <Status> element, with the attributes – and attribute values of both elements configured as specified herein or as specified in other specification(s) in the ID-WSF or ID-SIS specification sets.
ID-FF	The Identity Federation Framework (ID-FF) is the title for a subset of the Liberty specification suite which defines largely HTTP-based protocols for web single sign-on and identity federation.
ID-PP	The "ID Personal Profile" is an ID-SIS – based service which can provide profile information regarding Principals, typically subject to policy established by those Principals.
ID-SIS	Liberty Identity Service Interface specification set. ID-SIS-based services are identity services typically built on ID-WSF.
ID-WSF	Liberty Identity Web Services Framework specification set. An ID-WSF-based service is an identity service that is at least discoverable in principle and is based on the Liberty specifications for SOAP bindings and security mechanisms.

Identifier	A representation (for example, a string) mapped to a system entity that uniquely refers to it.
Identity	The essence of an entity. One's identity is often described by one's characteristics, among which may be any number of identifiers.
Identity provider (IdP)	A Liberty-enabled system entity that manages identity information on behalf of Principals and provides assertions of Principal authentication to other providers.
Identity service	In Liberty, an abstract notion of a web service whose operations are indexed by identity. Such a service might maintain information about, or on behalf of, identities or perform actions on behalf of identities.
Liberty-Enabled client or proxy (LECP)	A Liberty-enabled client is a client that has, or knows how to obtain, knowledge about the identity provider that the Principal wishes to use with the service provider. A Liberty-enabled proxy is an HTTP proxy (typically a WAP gateway) that emulates a Liberty-enabled client. Liberty-enabled Provider – An umbrella term referring to any Provider offering any ID-FF-, ID-WSF- or ID-SISbased services.
Liberty-Enabled Client and Proxy Profile	This profile specifies interactions between Liberty-enabled clients and/or proxies, service providers and identity providers [LibertyBindProf].
Liberty-enabled User Agent or Device (LUAD)	A user agent or device that has specific support for one or more profiles of the Liberty specifications. It should be noted that although a standard web browser can be used in many Liberty-specified scenarios, it does not provide specific support for the Liberty protocols and thus is not a LUAD. No particular claims of specific functionality should be implied about a system entity solely based on its definition as a LUAD. Rather, a LUAD may perform one or more Liberty system entity roles as defined by the Liberty specifications it implements. For example, a LUADLECP is a user agent or device that supports the Liberty LECP profile and a LUAD-DS would define a user agent or device offering a Liberty ID-WSF Discovery Service.
Markup Language	A set of XML elements and XML attributes to be applied to the structure of an XML document for a specific purpose. A markup language is typically defined by means of a set of XML schemas and accompanying documentation. For example, the Security Assertion Markup Language (SAML) is defined by two schemas and a set of normative SAML specification text.
Ordinary ID-* message	A Liberty Identity Web Services Framework (ID-WSF) or Service Interface Specification (ID-SIS) message. It is designed to be conveyed by essentially any transport or transfer protocol, notably SOAP. It is also known among the ID-* specifications as a service request or an ID-WSF (service) request or an ID-SIS (service) request.

Policy Decision Point (PDP)	A system entity that makes authorization decisions for itself or for other system entities that request such decisions. For example, a SAML PDP consumes authorization decision requests and produces authorization decision assertions in response. A PDP is an "authorization decision authority".
Policy Enforcement Point (PEP)	A system entity that requests and subsequently enforces authorization decisions. For example, a SAML PEP sends authorization decision requests to a PDP and consumes the authorization decision assertions sent in response.
Principal	A system entity whose identity can be authenticated. In Liberty usage, Principal is usually synonymous with a "natural person". A Principal's identity may be federated. Examples of Principals include individual users, groups of individuals, organizational entities, e.g., corporations, or a component of the Liberty architecture.
Principal Identity	A representation of a principal's identity, typically an identifier.
Privacy	In Liberty, proper handling of personal information throughout its life cycle, consistent with the preferences of the subject.
Profile	In SAML, a set of rules describing how to embed assertions into and extract them from a framework or protocol. Each profile is given a name in the pattern "xxx profile of SAML". In Liberty, a profile is data comprising attributes that may be maintained on behalf of a system entity (usually a Principal), over and beyond its various identifiers. At least some of this information (for example, addresses, preferences, and card numbers) is typically provided by the Principal.
Provider	A Liberty-enabled entity that performs one or more of the provider roles in the Liberty architecture – for example service provider or identity provider. Providers are identified in Liberty protocol interactions by their Provider IDs or optionally an Affiliation ID.
Relying Party	A system entity that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject.
Requester, SAML Requester	A system entity that utilizes the SAML protocol to request services from another system entity (a SAML authority, a responder). The term "client" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML requester is architecturally distinct from the initial SOAP sender.
Resource	a) Data contained in an information system (for example, in the form of files, information in memory, etc). b) A service provided by a system. SAML refers to resources by means of URI references.

Responder, SAML Responder	A system entity (a SAML authority) that utilizes the SAML protocol to respond to a request for services from another system entity (a requester). The term “server” for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the ultimate SOAP receiver.
Rights Expression Language (REL)	In Liberty, a Rights Expression Language facilitates the expression of who are the “rights holders” for a resource, who is authorized to use a resource and their applicable permissions, and any constraints or conditions imposed on such permissions. They also may express “rights entities” and “rights transactions”.
SAML Authority	An abstract system entity in the SAML domain model that issues assertions. See also attribute authority, authentication authority, and policy decision point (PDP).
Security	A collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity and availability. It is intended to ensure that a system resists potentially correlated attacks.
Security Architecture	A plan and set of principles for an administrative domain and its security domains that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services and the performance levels required in the elements to deal with the threat environment. A complete security architecture for a system addresses administrative security, communication security, computer security, emanations security, personnel security and physical security, and prescribes security policies for each. A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats. A security architecture should explicitly evolve over time as an integral part of its administrative domain’s evolution.
Security Assertion	An assertion that is scrutinized in the context of a security architecture.
Security Assertion Markup Language, SAML	The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP).

Security Domain	An environment or context that is defined by security models and security architecture, including a set of resources and set of system entities that are authorized to access the resources. One or more security domains may reside in a single administrative domain. The traits defining a given security domain typically evolve over time.
Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect resources. Security policies are components of security architectures. Significant portions of security policies are implemented via security services, using security policy expressions.
Security Policy Expression	A mapping of principal identities and/or attributes thereof with allowable actions. Security policy expressions are often essentially access control lists.
Security Service	A processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems, for example, an authentication service or a PKI-based document attribution and authentication service. A security service is a superset of authentication, authorization and accounting (AAA) services. Security services typically implement portions of security policies and are implemented via security mechanisms.
Security Token	In Liberty, a security token is a collection of security-related information that is used to represent and substantiate a claim. Outside of Liberty, the term “security token” often refers to hardware-based devices, e.g. so-called “token cards”. One should not confuse the latter and the former definitions. However, it is possible for some given authentication mechanism to employ token cards in the process of authentication.
Session	A lasting interaction between system entities, often involving a user, typified by the maintenance of some state of the interaction for the duration of the interaction.
Simple Authentication and Security Layer (SASL)	An approach to modularizing protocol design such that the security design components, e.g. authentication and security layer mechanisms, are reduced to a uniform abstract interface. This facilitates a protocol’s use of an open-ended set of security mechanisms, as well as a so-called “late binding” between implementations of the protocol and the security mechanisms’ implementations. This late binding can occur at implementation- and/or deployment-time. The SASL specification also defines how one packages authentication and security layer mechanisms to fit into the SASL framework, where they are known as SASL mechanisms, as well as register them with the Internet Assigned Numbers Authority for reuse.

Site	An informal term for an administrative domain in geographical or DNS name sense. It may refer to a particular geographical or topological portion of an administrative domain or it may encompass multiple administrative domains, as may be the case at an ASP site.
SSO Assertion, Single Sign-on Assertion	An assertion with conditions embedded that explicitly define its lifetime and include one or more statements about the authentication of a subject. Additional information about the subject, such as attributes, may also be included in the assertion.
Subject	A principal in the context of a security domain. SAML assertions make declarations about subjects.
System Entity	An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality.
Transport Layer Security Protocol (TLS)	An evolution of the SSL protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery.
Trusted Authority	In Liberty, a Trusted Third Party (TTP) which issues and vouches for assertions, otherwise known as an identity provider.
Trusted Third Party	In general, a security authority or its agent, trusted by other entities with respect to security-related activities. In the context of Liberty, these other entities are, for example, Principals and service providers and the trusted third party is typically the identity provider(s) involved in the particular interaction of interest
Ultimate SOAP Receiver	The SOAP receiver that is a final destination of a SOAP message. It is responsible for processing the contents of the SOAP body and any SOAP header blocks targeted at it. In some circumstances, a SOAP message might not reach an ultimate SOAP receiver, for example because of a problem at a SOAP intermediary. An ultimate SOAP receiver cannot also be a SOAP intermediary for the same SOAP message.
User	A natural person who makes use of a system and its resources for any purpose.
Uniform Resource Identifier (URI)	A compact string of characters for identifying an abstract or physical resource. URIs are the universal addressing mechanism for resources on the World Wide Web. Uniform Resource Locators (URLs) are a subset of URIs that use an addressing scheme tied to the resource's primary access mechanism, for example, their network "location".
URI Reference	A URI that is allowed to have an appended number sign (#) and fragment identifier. Fragment identifiers address particular locations or regions within the identified resource.

XML	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.
XML Attribute	An XML data structure that is embedded in the start-tag of an XML element and that has a name and a value. For example, the italicized portion below is an instance of an XML attribute: <Address AddressID="A12345">…</Address>. See also attribute.
XML Element	An XML data structure that is hierarchically arranged among other such structures in an XML document and is indicated by either a start-tag and end-tag or an empty tag. For example: <Address AddressID="A12345"> <Street>105 Main Street</Street> <City>Springfield</City> <State Or Province> <Full>Massachusetts</Full> <Abbrev>MA</Abbrev> </State Or Province> <Post Code="567890"/> </Address>
XML Namespace	A collection of names, identified by a URI reference, which are used in XML documents as element types and attribute names. An XML namespace is often associated with an XML schema. For example, SAML defines two schemas and each has a unique XML namespace.
XML Schema	The format developed by the World Wide Web Consortium (W3C) for describing rules for a markup language to be used in a set of XML documents. In the lowercase, a "schema" or "XML schema" is an individual instance of this format. For example, SAML defines two schemas, one containing the rules for XML documents that encode security assertions, and one containing the rules for XML documents that encode request/response protocol messages. Schemas define not only XML elements and XML attributes, but also data types that apply to these constructs.

11. APPENDIX - GOVERNANCE ROLES AND RESPONSIBILITIES

	Steering Committee	Federation Management Team	Identity Provider	Service Provider
Who / why?	This is the executive level body with representation from primary stakeholders that guides the federation and is the final authoritative body to make decisions for the federation	This is the body that manages the day-to-day operations of the Federation, including developing and maintaining standards, membership coordination and providing executive secretariat services to the Steering Committee.	An entity that vets individuals, collects attributes about these individuals, maintains these attributes in an accurate and timely manner. The IDP performs user authentication each time an individual presents themselves to the federation and assigns the current attributes about the individual for a given information technology session. These attributes are presented to Service Providers in the Federation or on a federation-to-federation basis	A federation member organization that provides one or more electronic information service(s) to the Federation. Service providers' services evaluate the set of Identity Provider attributes presented to the SP in a form that is consistent with the SICAM Interface Control Document (e.g. SAML assertion) to determine what access to provide or deny to each end user.
Activities/ Responsibilities		▪ Developing policies and guidelines pertaining to the definition and usage of the SICAM Metadata Specification standard for end-user attributes ▪ Implementing	▪ Identity Provider shall provide a trust model that ensures that an individual is linked to identities which have been issued, protected, and managed to	▪ Service providers shall have the capability to validate identity assertions that are submitted by the

	Steering Committee	Federation Management Team	Identity Provider	Service Provider
		approved processes for determining the membership of any new party in the SICAM ▪ Developing technical architecture and providing documents, including Interface Specifications, for technical interoperability within the SICAM ▪ Conducting day-to-day operational services, i.e., audits ▪ Defining Change Management processes for the SICAM ▪ Conducting interoperability testing of candidate commercial products, schemes or protocols ▪ Reviewing the conformance of the applicants to membership standards, including IDPs' mapping of their local policies and user attributes into SICAM standard attributes and SPs' mapping of their local access control policies into Boolean logic based on SICAM standard	provide the accuracy of asserted attributes. ▪ Identity Provider shall develop and provide an authentication process by which the user provides evidence to the identity provider, who independently verifies that the user is who he or she claims to be. ▪ Identity Provider shall develop a process to periodically reevaluate the status of the user and the validity of his or her associated identity. ▪ Identity Provider shall develop a process for attribute management to ensure the timely cancellation or modification of attributes should the user's status change. ▪ Identity Provider shall develop a process for auditing the attribute identification process, including	Federation Identity Providers (IDP) as part of a service request ▪ Service providers shall have the ability to define attributes that IDPs must present for access to the service. ▪ Service providers shall have the capability to react to receipt of various requestor assertions based on the established policy. ▪ Service providers shall provide audit services and make them available upon request to the federation. ▪

	Steering Committee	Federation Management Team	Identity Provider	Service Provider
		attributes ▪ Management and implementation of accepted SICAM standards and protocols operating within the SICAM ▪ Accountability authority and ensuring validity of the documents of the SICAM ▪ Facilitating the roles, relationships and mutual obligations of all parties operating in the SICAM ▪ Coordinate help desk efforts and provide engineering support ▪ Provide administrative support for the Board of Directors	registration activities, to ensure attributes are maintained in accordance with the process specified by that Identity Provider. Auditing must be conducted in a manner to identify any irregularities or security breaches. Audit information must be made available to the federation upon request. ▪ Identity Provider shall provide a process to assist users who have either lost or forgotten their means of authentication. ▪ Identity Provider shall adhere to the problem resolution process in SICAM Policies and Procedures Guidelines.	

12. APPENDIX - SERVICE PROVIDER TRUST AGREEMENT

The GIFPM framework provides the following examples of trust agreements. They are included in GIFPM Governance Guidelines Working Draft v0.95

Source: http://it.ojp.gov/docdownloader.aspx?ddid=1079

Service Provider Agreement

In order to allow for the connection of multiple parties in an electronic information sharing trust environment, The _____ (insert federation name) Federation (—the Federation||), allows for the interconnection of separately-provided identities, associated with end users, and services for those users

Therefore,
This Service Provider Agreement (the —SP Agreement||) is being entered into by the Federation Management and _____ (insert authorized organization name), the Service Provider. The purpose of the SP Agreement is to memorialize the intent of the Service Provider to provide services to the Federation and for the Federation Management to allow the Service Provider access to the Federation infrastructure to unite Identity Provider end-users and the Service Provider's services.

Service Provider Role
The Service Provider agrees to provision its services in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines. These services will be accessible to Identity Provider end-users who meet the requirements of an established and documented access policy that the Service Provider has defined. Unless the Service Provider has specifically identified certain or all of the Service Provider's services as not public, the Federation may publicize the services which the Service Provider has made available to the Federation.
However, Service Providers who need to keep confidential the availability of their service(s), may specify the set of required attributes for discovery of their Services in the Federation directory of services. At all times that the Service Provider is a party to this agreement it agrees to abide by Specifically the Service Provider agrees to meet minimum security and availability standards. The Service Provider agrees to comply with any decisions made through the governance process, in accordance with the Global Federated Identity and Privilege Management Governance Guidelines

1. Service providers shall have the capability to validate identity assertions that are submitted by the Federation Identity Providers (IDP) as part of a service request.
2. Service providers shall have the ability to define attributes that IDPs must present for access to the service.
3. Service providers shall have the capability to react to receipt of various requestor assertions based on the established policy.
4. Service providers shall provide audit services and make them available upon request to the federation.

All service providers must certify that they are only providing information or services that they have legal rights to provide. Consumers of a federation service are obligated to comply with the specific service-level policies governing the appropriate use, handling, dissemination and/or destruction of the information accessed. The user obligations specified by a specific service policy is not in the scope of the Federation governance.

Federation Role
The Federation Management agrees that it will provide the Service Provider with the operational support to enable the Identity Providers' end-users and the Service Provider's services to interact. The Federation Management agrees that it will abide by the Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP] and that it will make governance decisions in accordance with GFIPM Governance Guidelines [GFIPM GOV].

Personally Identifiable Information
All Service Providers must manage their information service privacy data in accordance with their service specific privacy policies. All identity attributes received by the service provider from Identity Providers can only be used to make authorization decisions, dynamically provision accounts, and perform audit logging.

Termination
Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP], upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

Modification of Agreement
A modification of this agreement proposed by the Federation Management or by the Service Provider will not be final unless it has been agreed to by both parties and approved by the Board of Directors in writing.

Waiver
A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management and the Board of Directors.

Assignment
This agreement may not be assigned, in whole or in part, by the Service Provider without the prior written consent of the Federation Management and the Board of Directors.

Severability
If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradictory provision will be reviewed and then clarified or corrected by the Board of Directors.

Entire Agreement
This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

Federation Documents
The operation of the Federation is governed by the following documents, which are incorporated into this agreement by reference:

- The Global Federated Identity and Privilege Management Governance Guidelines [GFIPM GOV] – this document defines the roles and responsibilities of the Federation, the Federation Management, the Board of Directors, Service Providers, and Identity Providers.
- The Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP] – this document details the way in which the Federation policies will be carried out.
- GFIPM Interface Control Document [GFIPM ICD] – this document details the technical interfaces required to be part of the federation.
- GFIPM Metadata Specification Package [GFIPM METADATA] – this specification package details the metadata requirements that must be used as part of the federation.

Notices
All notices, certificates, acknowledgments or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management shall be delivered as follows: ____(insert address)_____

Notice to the Service Provider shall be delivered as follows: _____(insert address)_____

The following material, which has been submitted with this agreement, is incorporated in the agreement by reference: (insert list documents)

13. APPENDIX - IDENTITY PROVIDER TRUST AGREEMENT

The GIFPM framework provides the following examples of trust agreements. They are included in GIFPM Governance Guidelines Working Draft v0.95

Source: http://it.ojp.gov/docdownloader.aspx?ddid=1079

Identity Provider Agreement

In order to allow for the connection of multiple parties in an electronic information sharing trust environment, The _____ (insert federation name) Federation —the Federation‖) allows for the interconnection of separately provided identities, associated with end users, and services for those users.

Preamble

This Identity Provider Agreement (the —IDP Agreement) is being entered into by the Federation Management and _____ (insert authorized organization name), the Identity Provider. The purpose of the IDP Agreement is to memorialize the intent of the Federation Management to provide access to the federation systems to Identity Provider and Identity Provider end users, and for the Identity Provider to create, maintain, and manage identities of their respective end users.

Identity Provider Role

The role of the Identity Provider is to create, maintain, secure and manage the identities of their end users; and accurately assert those identities, and attributes about those identities, only to authorized Federation Service Providers (SP) in accordance with federation technical documents. In accomplishing this role, the Identity Provider agrees that it will adhere to a documented process for the initial vetting of their end users identity, for any changes, for the removal of end users, and for the ongoing management of users attributes. At all times that the Identity Provider is a party to this agreement it agrees to abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP]. Specifically the Identity Provider agrees to meet minimum security and availability standards and at a minimum should do the following:

1. Identity Provider shall provide a trust model that ensures that an individual is linked to identities which have been issued, protected, and managed to provide the accuracy of asserted attributes.
2. Identity Provider shall develop and provide an authentication process by which the user provides evidence to the identity provider, who independently verifies that the user is who he or she claims to be.
3. Identity Provider shall develop a process to periodically reevaluate the status of the user and the validity of his or her associated identity.
4. Identity Provider shall develop a process for attribute management to ensure the timely cancellation or modification of attributes should the user's status change.
5. Identity Provider shall develop a process for auditing the attribute identification process, including registration activities, to ensure attributes are maintained in accordance with the process specified by that Identity Provider. Auditing must be conducted in a manner to

identify any irregularities or security breaches. Audit information must be made available to the federation upon request.

6. Identity Provider shall provide a process to assist users who have either lost or forgotten their means of authentication.
7. Identity Provider shall adhere to the problem resolution process in Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP].

Federation Role

The Federation Management agrees that it will provide the Identity Provider and their end users access to the federation systems. The Federation Management agrees that it will abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP] and that it will make governance decisions in accordance with the Federated Identity and Privilege Management Governance Guidelines [GFIPM OPP].

Personally Identifiable Information (PII)

Identity Providers assert identity attribute data, including PII attributes, as necessary to meet the authorization requirements of Service Providers, for audit logs and for supporting dynamic account provisioning. IDP attributes, including PII attributes, shall 740 not be used for any other business purposes.

Termination

Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures [GFIPM OPP], upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

Modification of Agreement

A modification of this agreement proposed by the Federation Management or by the Identity Provider will not be final unless it has been agreed to by both parties and approved by the Board of Directors in writing

Waiver

A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management and the Board of Directors.

Assignment

This agreement may not be assigned, in whole or in part, by the Identity Provider without the prior written consent of the Federation Management and the Board of Directors.

Severability

If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradictory provision will be reviewed and then clarified or corrected by the Board of Directors.

Entire Agreement
This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

Federation Documents
The operation of this Federation is governed by the following documents, which are incorporated into this agreement by reference: The Global Federated Identity and Privilege Management Governance Guidelines [GFIPM GOV] – this document defines the roles and responsibilities of the Federation, the Federation Management, the Board of Directors, Service Providers, and Identity Providers. Global Federated Identity and Privilege Management Operational Standards Policies and Procedures Guidelines [GFIPM OPP] – this document details the way in which the federation policies will be carried out. Global Federated Identity and Privilege Management Interface Control Document [GFIPM ICD] – this document details the technical interfaces required to be part of the federation. Global Federated Identity and Privilege Management Metadata Specification [GFIPM METADATA] – this document details the metadata requirements that must be used as part of the federation.

Notices
All notices, certificates, acknowledgments or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management shall be delivered as follows:

____(Insert address)_____ _____
_____
Notice to the Identity Provider shall be delivered as follows:
____(Insert address)_____ _____
_____
The following material, which has been submitted with this agreement, is incorporated in the agreement by reference:
(List documents)

Signatures
By signing below _____ (authorized organization name), the Identity Provider, certifies that they have read this document, that it is accurate and agrees to abide by this agreement and all Federation documents referenced herein.
_____ (authorized organization name),
the Identity Provider By:
_____ (authorized representative)
_____ (title)Signature
By signing below _____ (insert authorized organization name) , the Service Provider, certifies that they have read this document, that it is accurate and agrees to abide by this agreement and all Federation documents referenced herein.
_____ (insert authorized organization name),

the Service Provider By:
_____ (signature of authorized representative) _____ (insert title)

14. APPENDIX - ASSURANCE LEVEL DEFINITIONS AND EXAMPLES

Assurance Level Classifications		
Level	Description	Examples
1	Little or no confidence in the asserted identity's validity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.	A. the submission of forms by individuals in an electronic transaction will be a Level 1 transaction: (i) when all information is flowing to the Federal organization from the individual, (ii) there is no release of information in return, and (iii) the criteria for higher assurance levels are not triggered. For example, if an individual applies to a Federal agency for an annual park visitor's permit (and the financial aspects of the transaction are handled by a separate contractor and thus analyzed as a separate transaction, the transaction with the Federal agency would otherwise present minimal risks and could be treated as Level 1. B. A user presents a self-registered user ID or password to the U.S. Department of Education web page, which allows the user to create a customized "My.ED.gov" page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal. C. A user participates in an online discussion on the colorado.gov website, which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.
2 Federal Bridge Certification Authority (FBCA) Basic Level	Some confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to	A. A user subscribes to the Gov Online Learning Center (www.golearn.gov). The site's training service must authenticate the person to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student's privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.

	any state action)	B. A beneficiary changes her address of record through the Department of Human Services web site. The site needs authentication to ensure that the entitled person's address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary's address of record, it entails moderate risk of unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication. C. An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate. D. An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create moderate potential impact for unauthorized release, but the system's security measures reduce the overall risk to low. E. A first responder accesses a disaster management reporting web site to report an incident, share operational information, and coordinate response activities. Department of Homeland Security has established that the default assurance level for first responders be at Level 2 or higher.
3 FBCA Medium Level	A high degree of confidence in the asserted identity's validity. This level is relevant to environments where risks	????A team electronically submits a bidder's confidential information to the State AG Office for review. Improper disclosure would give competitors a competitive advantage. B. A supplier maintains an account with the Department of Personnel & Administration's

	and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving private information where access by individuals with malicious intent would result in significant harm.	Contracting Officer for a large state procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate. C. An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. Her access to PII creates moderate potential impact for unauthorized release. If technical controls (such as a virtual private network) are in place to limit system access to the agency premises, this could be level 2. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.
4 FBCA Medium (Hardware) or High Level	A very high degree of confidence in the asserted identity's validity. Users may present Level 4 credentials to assert identity and gain access to highly restricted system or physical resources, without the need for further identity assertion controls. This level is appropriate for use where the threats to data are high, or the consequences of thee failure of security services are severe. This may include very high value transactions or high levels of fraud risk.	????A Colorado State Patrol official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations. B. A Department of Corrections pharmacist dispenses a controlled drug. The Department would need full assurance that a qualified doctor prescribed it. The Department is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount. C. Agency investigators use a remote system giving them access to potentially sensitive personal client information. Using their laptop at client worksites, personal residences, and businesses, they accesses information over the Internet via various connections. Federal statutes require "securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them."

15. APPENDIX - IDENTITY PROOFING REQUIREMENTS BY ASSURANCE LEVEL

	In-Person	Remote
Level 1	Minimum Requirements	
	There are no level-specific requirements at Level 1	
Level 2	Minimum Requirements	
	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport). Enrolling official: ▪ Inspects photo-ID, compare picture to applicant, record ID number, address and DOB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number. Enrolling official: ▪ Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DOB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. ▪ Initiate address confirmation and notification: a) Send notice to the address of record confirmed by the records check; or b) Issue credentials in a manner that confirms the address of record supplied by the applicant; or ▪ Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or email at the number or email address indicated by the applicant's records.
Level 3	Minimum Requirements	

	Possession of a verified current primary government photo ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport). Enrolling official: ▪ Inspect Photo ID and verify via the issuing organization or through credit bureaus or similar databases. Confirm that name, DOB, address, and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DOB. If ID is valid and photo matches applicant then: a) if ID confirms address of record, authorize or issue credentials and send notice to address of record; b) if ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Possession of a valid government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number. Enrolling official: ▪ Verify information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar data bases, and confirm that: name, DOB, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. ▪ Address confirmation: a) Issue credentials in a manner that confirms or independently verifies the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records while recording the applicant's voice.
Level 4	Minimum Requirements	

	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application Enrollment Official: ▪ Primary Photo ID: Inspect photo ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and DOB. ▪ Secondary Government ID or Financial Account: a) Inspect photo ID and if apparently valid, compare picture to applicant, record ID number, address, and DOB; or b) Verify financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that; name, DOB, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. ▪ Record Current Biometric: record a current biometric (e.g., photo, fingerprint, or other) to ensure that applicant cannot repudiate application. ▪ Confirm Address: issue credentials in a manner that confirms address of record. ▪ Conduct appropriate background check if required.	Not Applicable

16. APPENDIX - GENERIC USAGE PATTERNS

This appendix described the user interaction during federated identity interactions. The examples listed here are examples of identity federations involving several trusted partners. Other examples and more complex examples will emerge during the deployment of a SICAM architecture.

SICAM Basic Usage Pattern

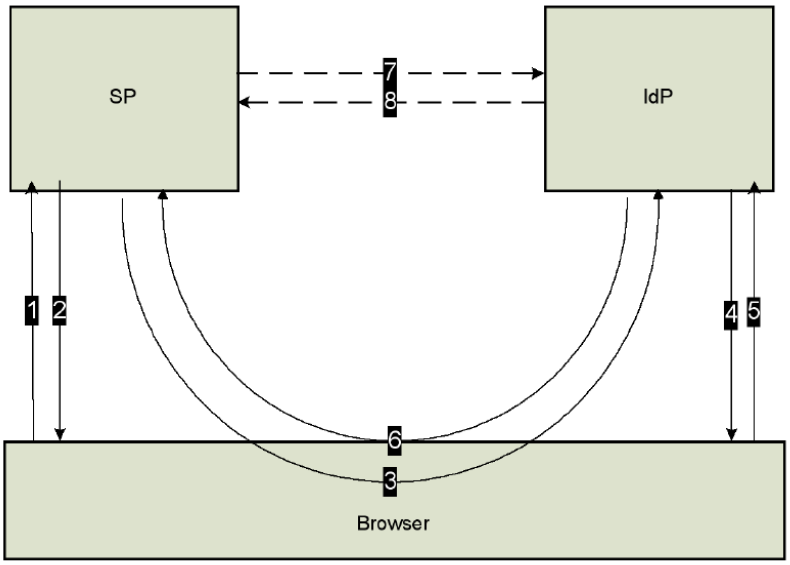


Figure 4 – SICAM Generic Usage Pattern

The summarized communication flow for the generic usage pattern is:

1. The service user attempts to access a resource at an SP department website.
2. The SP department may place a session cookie or similar object on the service user's browser to establish the local authentication session
3. The SP department's service user is redirected via their web browser to a logon page.
4. The IdP department presents the web user with a logon page.
5. SP department's service user submits logon information on the logon page.

The IdP department will respond to the SP department with a message via the service user's browser. The message contains either an assertion or an artifact, depending on the SAML binding used. Where the message contains an assertion (i.e. POST binding), the SP department uses the assertion to authenticate the service user using its own internal processes and the pattern is complete. Where the message contains an artifact (i.e. Artifact binding), the SP department dereferences the artifact to determine the IdP and continues with Step 7

.

1. Where the message contains an artifact, the SP includes the artifact in a request (such as an application-to-application digitally-signed SOAP message based Web Services call) to the IdP via a 'back channel' (such as an appropriately secured SSL/TLS leased data connection or Virtual Private Network) to receive the assertion.
2. The IdP resolves the request by sending a message with the assertion reserved for the artifact via the mechanism described in (7) above.

In SICAM model the following design and business principles should apply:

- **No reliance on the security of the service user's personal computer** – Due to the difficulty in securing every personal computer (PC) on the Internet, no reliance can be placed upon the service user's PC for the transport of authentication-related messages and for installing client-side authentication software (with the exception of multi-factor authentication software applications).
- **Federated identifier –** Service users who logon at the authentication provider website must be given something (a unique federated identifier) that they can present to service provider department websites as confirmation that they have been successfully authenticated.
- **State persistence** – If the service user goes to the department SP website and encounters a step(s) in a service that requires the service user to be authenticated, the service user must be redirected to the authentication provider department website. The redirection process and application logic must be implemented in such a way that the authentication provider department website will redirect the service user back to the service provider department website once they have authenticated, bearing their authentication credential, 'handle' and session ID. The service provider department website must then be able to seamlessly resume the interrupted service step.
- **Verified federated identifier** – The effort to compromise the security of the authentication credential must be prohibitive. The service provider department website must be able to verify that the credential was issued by some party that the service provider department website trusts. Typically this is achieved using digital certificates for the servers involved in the exchange.

- **Verified messages** – The effort to compromise the security of any messages, or fragments of messages, that support the above requirements must be prohibitive. The service provider department website and authentication provider department website must be able to verify that the messages were issued by a party within the federation of websites. Typically this is achieved by signing and/or encrypting the message parts.
- **Universal services** – Any service provider department with an online presence and seeking to authenticate their service users on the Internet must be able to participate in the federation.
- **Audit Trail** – Security assertion sessions must have an accompanying audit trail.
- **Archive management** – Establish practices for managing archives containing signed or encrypted data. Examples of potential issues are:
  - Logs that contain information that was signed with certificates that have since expired may be difficult to validate. Without trusted timestamps it would be unclear whether the signed object was created before the certificate was revoked or expired.
  - Encrypted elements in the logs will likely require the private key of the recipient to decrypt. If those keys have not been archived it may be impossible to read the old logs.

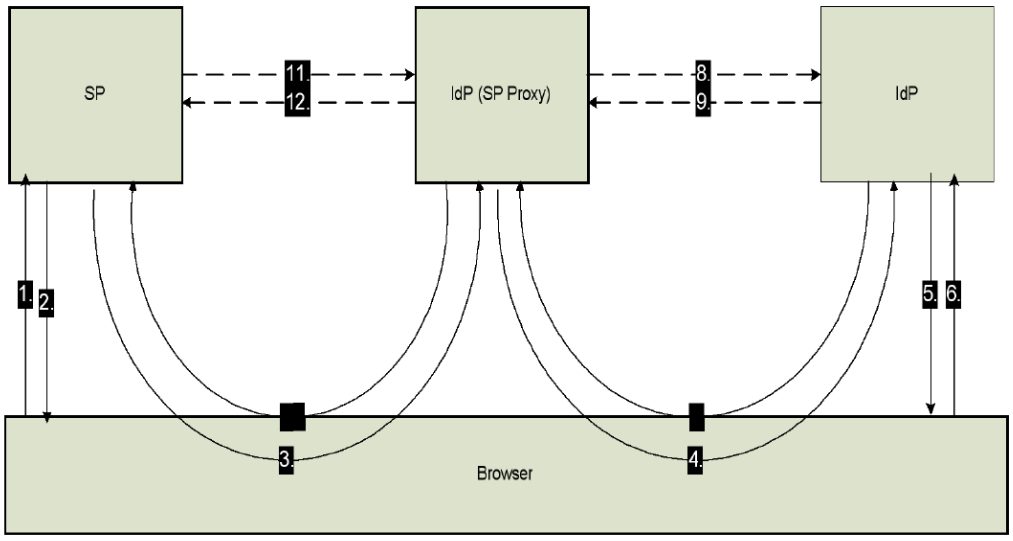


Figure 5 – SICAM IdP Proxy Usage Pattern

The profile depicted in Figure 5 is a variation on the generic SAML v2.0 Web Browser SSO profile11. It describes how an IdP contacted by an SP acts in the role of an SP (i.e. proxies) to a different (endpoint) IdP where the service user ultimately authenticates. The endpoint IdP returns an assertion that is used by the proxying IdP to build a new assertion for the originating SP to use.

The use pattern reflecting this profile emerged from a number of agencies that expect to use the GLS (the endpoint IdP) for the act of authenticating, while managing all other aspects of the service user's session – SSO, authorization and provisioning, identity attributes etc.

[11] NOTE – IdP Proxy is not explicitly detailed in the OASIS SAML v2.0 Profiles Specification. However it is featured in the OASIS SAML v2.0 Conformance Requirements (Table 3 'Extended IdP, SP' p 10, lines 187-188).

17. APPENDIX - EXAMPLE OF IDENTITY ATTRIBUTES

	Individual	Employee	First Responder
Attribute Name	Classification	Classification	Classification
Given Name	1	1	1
Middle Name	1	1	1
Sur Name	1	1	1
NameSuffix Text	1	1	1
Sex Code	1	1	1
Organization Association Category		1	1
Organizational Affiliation		1	1
Photo	1	1	1
Card Expiration Date			1
Card Issue Date			1
Employee Rank Text			1
Cardholder Unique Identifier		1	
Fingerprint Image	1	1	1
Digital Signature Certificate			1
Key Management Certificate			1
Card Authentication Certificate			1
Card Holder ID Status			1
Card Holder ID Status Date			1
Telephone Number	2	2	2
Birth Date	2	2	2
Citizenship FIPS10-4 Code	2	2	2
US Citizenship	2	2	2
Security Clearance Code		2	2
Clearance Date		2	2
Clearing Agency		2	2
Card Status			1
Card Status Date			1

	Individual	Employee	First Responder
Attribute Name	Classification	Classification	Classification
Designated Role		2	2
Certification Type			2
Certification Name			2
Certification Date			2
Certifying Authority			1
Emergency Contact Person GivenName			3
Emergency Contact Person SurName			3
Emergency Contact Telephone Number			3
Emergency Contact Email			3
Driver License Number	2	2	2
DL Expiration Date	2	2	2
Social Security Number	3	3	3
Mailing Address	3	3	3
Mailing Address City	2	2	2
State	2	2	2
Zip Code	2	2	2
Residence Address (if different than mailing address)	3	3	3
City	2		
State	2		
Zip Code	2		
Hair Color	3		
Eye Color	3		
Height	3		
Weight	3		
License Class	2		
Also Known As (AKA) Names	1		
Out of State DL Number	2		
Out of State	2		

	Individual	Employee	First Responder
Attribute Name	Classification	Classification	Classification
Physical & Mental Condition	3		
Medical Information	3		
License Restrictions, Endorsements and Certificates	2		

18. APPENDIX - BIBLIOGRAPHY

Several sources pf publically available information was used in the creation of this document. The following is a list of several of those sources.

U.S. Department of Justice's, Global Federated Identity and Privilege Management (GFIPM), Governance Guidelines -- Working Draft Version 0.95 - http://it.ojp.gov/docdownloader.aspx?ddid=1079

U.S. Department of Justice's, Global Federated Identity and Privilege Management (GFIPM), Operational Policies and Procedures -- Working Draft Version 0.95 - http://it.ojp.gov/docdownloader.aspx?ddid=1080

Global Federated Identity and Privilege Management (GFIPM) Metadata Specification Version 1.0 – http://www.it.ojp.gov/documents/GFIPM-Metadata-1.0.zip

Global Federated Identity and Privilege Management (GFIPM) Executive Summary - http://www.it.ojp.gov/documents/GFIPM_flyer.pdf

Global Federated Identity and Privilege Management (GFIPM) Security Interoperability Demonstration Project Report http://www.it.ojp.gov/documents/GFIPM_Security_Interoperability_Demonstration_Project_Report_2007-08-30.pdf

National Strategy for Trusted Identities in Cyberspace - http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance - http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf
"NIST Special Publication 800-63 - Electronic Authentication Guideline" - csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

"NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems" – http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

M-04-04:E-Authentication Guidance for Federal Agencies, OMB M-04-04 E-Authentication Guidance established 4 authentication levels. - http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

NIST SP 800-116 defines PIV credentials based Identity assurance levels for Uncontrolled/Controlled/Limited/Exclusion areas. - http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

"ACCESS CONTROL IN SUPPORT OF INFORMATION SYSTEMS SECURITY TECHNICAL IMPLEMENTATION GUIDE Version 2, Release 2" - 26 DECEMBER 2008 - http://iase.disa.mil/stigs/stig/access_control_stig_v2r2_final_26_dec_2008.pdf

"Introduction to the National Information Exchange Model (NIEM)" - http://www.niem.gov/files/NIEM_Introduction.pdf

"FIPS PUB 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors" - http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

FIPS PUB 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES - http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

"Federal Public Key Infrastructure (FPKI) Architecture Technical Overview" - http://www.idmanagement.gov/fpkia/documents/FPKIAtechnicalOverview.pdf

"Personal Identity Verification Interoperability For Non-Federal Issuers" - http://www.idmanagement.

“Identity Management Reference Architecture Practicum Report” by Paul Kavitz, Greg Black, Jay Ryan 3/17/2008

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation

Guidance V1.0 Published November 10,2009 - FCIOC and FEA

Federal Enterprise Architecture (FEA)

“Federated identity Management and Web Services Security” Axel Buecker, Werner Filip, Heather Hinton, Heinz Peter Hippenstiel, Mark Hollin, Ray Neucom, Shane Weeden, Johan Westerman
Rebooks
http://www.ibm.com/redbooks